

---

# **IT Security in the Age of Digitalization**

## **Toward an Understanding of Risk Perceptions and Protective Behaviors of Private Individuals and Managers in Organizations**

---



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

Am Fachbereich Rechts- und Wirtschaftswissenschaften  
der Technischen Universität Darmstadt

genehmigte

### **Dissertation**

von

Katja Rabea Sonnenschein, M.Sc.  
geboren am 17.12.1986 in Lauingen (Donau)

zur Erlangung des akademischen Grades  
Doctor rerum politicarum (Dr. rer. pol.)

Erstgutachter: Prof. Dr. Peter Buxmann  
Zweitgutachter: Prof. Dr. Alexander Benlian

Darmstadt 2018

Sonnenschein, Katja Rabea: IT Security in the Age of Digitalization – Toward an Understanding of Risk Perceptions and Protective Behaviors of Private Individuals and Managers in Organizations

Darmstadt, Technische Universität Darmstadt

Dissertation veröffentlicht auf TUpriints im Jahr 2018

Tag der mündlichen Prüfung: 06.03.2018

Veröffentlicht unter CC BY-SA 4.0 International

*<https://creativecommons.org/licenses/>*

## **Declaration of Authorship**

I hereby declare that the submitted thesis is my own work. All quotes, whether word by word or in my own words, have been marked as such.

The thesis has not been published anywhere else nor presented to any other examination board.

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht.

---

Katja Rabea Sonnenschein

Darmstadt, 16. Januar 2018

## **Abstract**

Nowadays, information technology (IT) has become an integral part of our everyday life. In both the private and business context, we extensively use different IT systems for data production, data organization, data analysis, and communication with others. Due to the extensive usage of IT, the amount of digitalized personal and organizational information is rapidly and incessantly rising — making both private individuals and organizations attractive targets for attackers. The necessity to effectively protect sensitive data from IT security incidents is highly discussed in practice and research, it attracts high media attention, and our society should be actually aware of the importance of IT security in today's digital world. However, recent reports demonstrate that organizations as well as private individuals — even though they are afraid of the rapid evolution of IT security risks — still often refrain from adopting the necessary IT security safeguards. To better prepare our society for the ongoing risks arising from extensive IT usage, a better understanding of how IT security is perceived by private individuals and managers is required.

Motivated by the findings and theoretical underpinnings from previous research, this thesis addresses several research questions with respect to IT security perceptions and behaviors of private individuals and managers in organizations. By conducting four studies — one among private individuals and three among managers in organizations — the thesis not only contributes to the current research but also provides useful recommendations for practice. Suppliers of IT and IT security products as well as managers in customer organizations can especially learn from the findings of the studies.

First, research paper A is focused on the private context and analyzes the gender differences in mobile users' IT security perceptions and protective behaviors. Drawing on Gender Schema Theory and Protection Motivation Theory, a mixed-method study (survey, experiment, and interviews) under laboratory conditions is conducted. The results show that IT security perceptions of females and males are based on different downstream beliefs and indicate that females are more likely to translate their intention to take precautionary actions into actual behavior than males.

The studies presented in research papers B, C, and D are conducted within the business context and focus on the IT security perceptions and behaviors of managers in organizations. Research paper B analyzes top managers' IT security awareness. Since previous research predominantly investigated IT security awareness at the employee level, a comprehensive conceptualization of IT security awareness at the management level is currently missing. To address this research gap, a structured literature review and expert interviews are performed in order to develop and test a comprehensive conceptualization — including both individual and organizational factors — of top managers' IT security awareness.

Within research paper C, managers' willingness to pay for IT security is in the focus of the investigation. Previous research largely neglected that various IT security safeguards might be differently evaluated by organizations, for example, due to different IT security requirements. By drawing on Kano's Theory, the study takes into account that — depending on the organization's individual IT security requirements — the implementation of IT security safeguards can also be associated with disadvantages. Based on interviews and an empirical study among managers, the study reveals that IT security safeguards are differently evaluated and that these different evaluations are associated with different levels of managers' willingness to pay.

Finally, research paper D analyzes managers' Status Quo-Thinking in risk perception. Based on Prospect Theory, Status Quo Bias research, and an empirical study among managers, the findings indicate that managers' risk evaluations and decisions to adopt new technologies are highly dependent on their assessments of the systems currently used in the organization. Moreover, the results implicate that the impact of Status Quo-Thinking on managers' risk assessments and intentions to adopt new technologies is stronger the less experienced a manager is with a new technology, probably resulting in an incorrect risk assessment and inappropriate adoption behavior.

Implications for research and practice are discussed in more detail within each research paper and summarized in the final chapter of the thesis.

## **Zusammenfassung**

Informationstechnologien (IT) sind längst integraler Bestandteil unseres alltäglichen Lebens. Sowohl im privaten als auch im beruflichen Kontext wird eine Vielzahl verschiedener IT-Systeme genutzt, um Daten zu produzieren, zu organisieren und zu analysieren sowie um mit Anderen zu kommunizieren. Infolge der stetig zunehmenden Integration von IT-Systemen in unseren privaten und beruflichen Alltag, wachsen die Anzahl und der Umfang digitalisierter Informationen rapide und stetig. Dies ist zwar mit Vorteilen verbunden, führt aber gleichzeitig dazu, dass Privatpersonen und Unternehmen zu attraktiven Zielen für Angreifer werden. Das Thema IT-Sicherheit genießt eine hohe Aufmerksamkeit in Forschung und Praxis, ist nahezu täglicher Bestandteil der medialen Berichterstattung und die Gesellschaft sollte sich längst über das Ausmaß der Bedrohungen durch IT-Sicherheitsrisiken bewusst sein. Dennoch zeigen aktuelle Statistiken, dass sowohl Unternehmen als auch Privatpersonen häufig darauf verzichten die erforderlichen Sicherheitsmaßnahmen umzusetzen. Um unsere Gesellschaft in Zukunft besser auf die kontinuierlich wachsende Gefahr vorbereiten zu können, wird ein tiefer gehendes Verständnis der Wahrnehmung von IT-Sicherheit durch Privatpersonen und Manager in Unternehmen benötigt.

Motiviert durch die theoretischen Grundlagen und die Ergebnisse vorheriger Forschung, werden in dieser Arbeit verschiedene Forschungsfragen im Hinblick auf die Wahrnehmung von IT-Sicherheit adressiert – einerseits aus der Perspektive von Privatpersonen und andererseits aus der Perspektive von Managern. Insgesamt wurden vier Studien durchgeführt und publiziert: eine Studie unter Privatpersonen und drei Studien unter Managern. Die Ergebnisse tragen zum aktuellen Stand der Forschung bei, liefern eine Basis für zukünftige Untersuchungen und ermöglichen das Ableiten wertvoller Handlungsempfehlungen für Privatpersonen und Praktiker. Insbesondere IT- und IT-Sicherheitsanbieter sowie Manager in Kundenunternehmen können von den Erkenntnissen profitieren.

Im Rahmen des ersten Forschungsartikels (Forschungspapier A) werden die Wahrnehmung von IT-Sicherheit und das daraus resultierende Verhalten unter Privatpersonen untersucht. Dabei steht, basierend auf den theoretischen Grundlagen der „Protection Motivation Theory“

und der „Gender Schema Theory“, die Analyse von geschlechterspezifischen Unterschieden im Fokus der Untersuchung. Die Ergebnisse der Studie (Fragebogen, Experiment und Interview) unter Smartphone-Nutzern zeigen, dass die Wahrnehmung von IT-Sicherheit bei Männern und Frauen auf unterschiedlichen kognitiven Prozessen basieren kann. Darüber hinaus weist die Studie darauf hin, dass Männer – im Gegensatz zu Frauen – dazu tendieren, sich nicht entsprechend ihrer Intention zu verhalten und häufig davon absehen entsprechende Sicherheitsmaßnahmen auch tatsächlich umzusetzen.

Die Studien der anderen drei Forschungsartikel (Forschungspapier B, C und D) wurden im Unternehmenskontext durchgeführt. Forschungspapier B analysiert das Bewusstsein für IT-Sicherheit von Topmanagern. Da die bestehende Forschung überwiegend das IT-Sicherheitsbewusstsein von Mitarbeitern untersucht, fehlt es derzeit an einer umfassenden Konzeptualisierung auf Ebene des Topmanagements. Um diese Forschungslücke zu schließen, wurde zunächst eine strukturierte Literaturrecherche durchgeführt und auf deren Basis eine Konzeptualisierung des IT-Sicherheitsbewusstseins von Topmanagern entwickelt, die sowohl individuelle als auch unternehmensbezogene Faktoren umfasst. Anschließend wurde die entwickelte Konzeptualisierung mithilfe von Experteninterviews validiert und angepasst.

In Forschungspapier C steht die Zahlungsbereitschaft für IT-Sicherheitsmaßnahmen im Fokus. In der bestehenden Forschung wurde bisher nur unzureichend berücksichtigt, dass IT-Sicherheitsmaßnahmen – z. B. aufgrund von individuellen IT-Sicherheitsanforderungen eines Unternehmens – von verschiedenen Managern unterschiedlich bewertet werden können. Um dies zu adressieren, wurde die in der Marketingforschung etablierte „Kano Theorie“ herangezogen und auf den IT-Sicherheitskontext angepasst. Die Ergebnisse der Interviews und der empirischen Studie unter Managern in Unternehmen lassen erkennen, dass IT-Sicherheitsmaßnahmen von verschiedenen Managern unterschiedlich bewertet werden können und dass diese unterschiedlichen Bewertungen zu divergierenden Zahlungsbereitschaften führen.

Schließlich wird in Forschungspapier D, basierend auf den theoretischen Grundlagen der „Prospect Theory“ und bestehender „Status Quo Bias“-Forschung, das Status-Quo-Denken von Managern bei der Risikowahrnehmung untersucht. Die Ergebnisse der empirischen Studie unter Managern in Unternehmen zeigen, dass die Risikobewertung und die Entscheidung eine neue Technologie zu adoptieren stark von der Wahrnehmung der derzeit genutzten IT-Systeme beeinflusst wird. Darüber hinaus weisen die Ergebnisse darauf hin,

dass dieses Status-Quo-Denken einen stärkeren Einfluss auf die Bewertung einer Technologie und die damit verbundene Adoptionsintention hat, je weniger Erfahrung ein Manager mit der betrachteten Technologie aufweist. Die Unsicherheit, welche mit fehlender Erfahrung einhergeht, kann dazu führen, dass Manager ihre verfügbaren Erfahrungen mit bereits bestehenden Technologien heranziehen. Dies kann wiederum eine verzerrte Risikowahrnehmung und das Treffen nachteiliger Entscheidungen mit sich bringen.

Die praktischen und theoretischen Implikationen werden in jedem Forschungspapier ausführlich diskutiert und im letzten Kapitel der vorliegenden Arbeit zusammengefasst.



## Acknowledgements

This thesis was written during my work as a research assistant at the Chair of Information Systems | Software Business and Information Management at the Technische Universität Darmstadt, Germany. The progress and completion of my dissertation would not have been possible without the support of many people, whom I sincerely thank with the following acknowledgements.

First, I am especially grateful to my supervisor Prof. Dr. Peter Buxmann, who greatly supported me and encouraged me in preparing and completing this thesis. I also want to express my deepest gratitude to Dr. André Loske for his great support, his valuable feedback on my research, and the trusting and enthusiastic collaboration in our joint research projects. A special appreciation also goes to Margareta Heidt for her fantastic feedback and the constructive teamwork. I am also very thankful to Prof. Dr. Alexander Benlian, who accepted the co-supervision of my thesis.

I sincerely thank my friends and colleagues Adrian, Alexander, Amina, Christian, Christoph, Helena, Hendrik, Jin, Katrin, Markus, Martin, Nicole, Nihal, Nora, Olga, Ruth, Stefan, Thomas, and Torben with whom I had many interesting and fruitful discussions and who provided valuable feedback on my research.

Furthermore, I want to express my gratitude to the House of IT e.V. for granting me a PhD scholarship.

Finally, I would like to express my sincere gratitude to my beloved partner, friends, sister, and especially to my parents for their invaluable support and thoughtfulness. They all gave me the strength to persist through challenging times.

## Table of Contents

<b>List of Figures .....</b>	<b>X</b>
<b>List of Tables.....</b>	<b>XI</b>
<b>List of Abbreviations.....</b>	<b>XIII</b>
<b>1.....Introduction .....</b>	<b>1</b>
1.1 Motivation and Problem Description.....	1
1.2 Objectives and Research Questions .....	4
1.3 Structure of the Thesis .....	7
<b>2.....Fundamentals .....</b>	<b>10</b>
2.1 IT Security Objectives .....	10
2.2 Risk Perception .....	10
2.3 Research Design and Methods.....	12
<b>3.....Research Paper A: Gender Differences in IT Security Appraisals and Protective Actions.....</b>	<b>15</b>
3.1 Introduction.....	16
3.2 Theoretical Background and Hypothesis Development.....	18
3.2.1 Protection Motivation Theory.....	18
3.2.2 Gender Schema Theory .....	20
3.2.3 Gender Differences in Appraisals and Coping Behaviors of Mobile Users .....	21
3.3 Research Methodology .....	25
3.3.1 Research Approach.....	25
3.3.2 Sampling.....	29
3.3.3 Data Analysis and Results .....	30
3.4 Discussion .....	36

3.5	Limitations and Future Research .....	42
<b>4.....</b>	<b>Research Paper B: Top Managers' IT Security Awareness.....</b>	<b>44</b>
4.1	Introduction.....	45
4.2	Step 1: Development of Conceptualization .....	48
4.2.1	Overview of Related Literature Streams .....	48
4.2.2	Literature Review on Top Managers' IT Security Awareness .....	49
4.2.3	Conceptualization of Top Managers' IT Security Awareness and Proposition Development.....	51
4.3	Step 2: Evaluation of the Conceptualization of Top Managers' IT Security Awareness .....	56
4.3.1	Research Approach.....	56
4.3.2	Qualitative Data Analysis .....	58
4.4	Discussion .....	66
4.5	Limitations and Future Research .....	68
4.6	Conclusion .....	70
<b>5.....</b>	<b>Research Paper C: Decision Makers' Willingness To Pay for IT Security .....</b>	<b>71</b>
5.1	Introduction.....	72
5.2	Theoretical Background and Research Hypotheses.....	73
5.2.1	Kano's Theory of Attractive Quality .....	73
5.2.2	Hypothesis Development.....	75
5.3	Research Methodology and Data Analysis .....	78
5.3.1	IT Security Safeguard Identification .....	78
5.3.2	Questionnaire Development and Quantitative Study.....	79
5.3.3	Statistical Analysis and Results .....	80
5.4	Discussion .....	87
5.5	Limitations, Future Research, and Conclusion .....	89
<b>6.....</b>	<b>Research Paper D: Managers' Status Quo-Thinking.....</b>	<b>91</b>
6.1	Introduction.....	92
6.2	Theoretical Background and Hypothesis Development.....	94

6.2.1 Technology Adoption Models and Rational Choice.....	94
6.2.2 Prospect Theory, Status Quo Bias, and Hypothesis Development .....	95
6.3 Research Methodology and Data Analysis .....	99
6.3.1 Survey Administration and Sample Characteristics .....	99
6.3.2 Assessment of Measurement Validations .....	103
6.3.3 Data Analysis and Results .....	104
6.4 Discussion.....	107
6.5 Limitations, Future Research, and Conclusion .....	110
<b>7.....Summary of Key Findings and Thesis Conclusion .....</b>	<b>113</b>
7.1 Theoretical Implications .....	113
7.2 Practical Implications.....	116
<b>References .....</b>	<b>119</b>

## List of Figures

Figure 1: Structure of the Thesis .....	7
Figure 2: Overview of Research Design and Methods in the Thesis .....	13
Figure 3: Research Model (Research Paper A) .....	25
Figure 4: Research Approach (Research Paper A) .....	26
Figure 5: Control Groups in the Experiment .....	29
Figure 6: Research Approach (Research Paper B) .....	47
Figure 7: Framework for Literature Reviewing (based on Vom Brocke et al. 2009) .....	49
Figure 8: Conceptualization of Top Managers' IT Security Awareness .....	65
Figure 9: Research Approach (Research Paper C) .....	79
Figure 10: Impact on Satisfaction and Dissatisfaction .....	86
Figure 11: Research Model (Research Paper D) .....	99
Figure 12: Data Analysis .....	105

## List of Tables

Table 1: Items Used in the Quantitative Study .....	27
Table 2: Demographic Sample Characteristics .....	30
Table 3: Indicator Reliability .....	31
Table 4: Quality Criteria for the Constructs and Fornell-Larcker Criterion Analysis .....	32
Table 5: Collinearity Statistics .....	32
Table 6: Classification of Actual Problem-Focused Coping Behavior .....	34
Table 7: Results of Structural Model Testing .....	35
Table 8: Overview of the Literature Search Process .....	50
Table 9: Factors of Top Managers' IT Security Awareness .....	54
Table 10: Descriptive Information for Interviewed Experts .....	57
Table 11: Structure of Interviews .....	57
Table 12: Coding Categories .....	58
Table 13: Characteristics of the IT Security Safeguard Categories .....	77
Table 14: IT Security Safeguard Evaluation Table .....	81
Table 15: Results of the IT Security Safeguard Categorization .....	81
Table 16: Results for the Group Variables .....	83
Table 17: Results for Different Levels of WTP within the IT Security Safeguard Categories .....	83
Table 18: Descriptives for Customers' WTP .....	83
Table 19: Impact on Customer Satisfaction .....	86
Table 20: Overview of Constructs .....	100
Table 21: Overview of Sample Characteristics .....	102
Table 22: Segmentation of Industry Sectors .....	102

---

Table 23: Assessment of Measurement Model .....	104
Table 24: Results of the Variance Model Estimation .....	106
Table 25: Results of the Multi-Group Analysis .....	107

## List of Abbreviations

<b>AIS</b>	Association on Information Systems
<b>AISeL</b>	Association on Information Systems Electronic Library
<b>AMCIS</b>	Americas Conference on Information Systems
<b>AVE</b>	Average Variance Extracted
<b>CA</b>	Cronbach's Alpha
<b>CD</b>	Customer Dissatisfaction
<b>CEO</b>	Chief Executive Officer
<b>CIO</b>	Chief Information Officer
<b>CIA</b>	Confidentiality, Integrity, and Availability
<b>CISO</b>	Chief Information Security Officer
<b>CR</b>	Composite Reliability
<b>CRM</b>	Customer Relationship Management
<b>CS</b>	Customer Satisfaction
<b>ECIS</b>	European Conference on Information Systems
<b>ERP</b>	Enterprise Resource Planning
<b>HICSS</b>	Hawaii International Conference on System Sciences
<b>ICIS</b>	International Conference on Information Systems
<b>IDC</b>	International Data Corporation
<b>IS</b>	Information Systems
<b>IT</b>	Information Technology
<b>MGA</b>	Multi-Group Analysis



---

<b>MIS</b>	Management of Information Systems
<b>OTA</b>	Online Trust Alliance
<b>PACIS</b>	Pacific Asia Conference on Information Systems
<b>PLS</b>	Partial Least Square
<b>PMT</b>	Protection Motivation Theory
<b>RQ</b>	Research Question
<b>SaaS</b>	Software as a Service
<b>SETA</b>	Security Education, Training, and Awareness
<b>SIGSVC</b>	Special Interest Group on Services in the AIS
<b>TAM</b>	Technology Acceptance Model
<b>TPB</b>	Theory of Planned Behavior
<b>TRA</b>	Theory of Reasoned Action
<b>UTAUT</b>	Unified Theory of Acceptance and Use of Technology
<b>VIF</b>	Variance Inflation Factor
<b>WTP</b>	Willingness To Pay

# 1 Introduction

## 1.1 Motivation and Problem Description

We are living in the age of digitalization, which is characterized by keywords like *Industry 4.0*, *Internet of Things*, *Cloud Computing*, and *Big Data*. By now, information technology (IT) is an integral part of both our private and professional everyday life. For example, from an organization's perspective, new IT developments frequently provide new opportunities to optimize business and production processes, to reduce cost and time investments, or to develop completely new business models. In many industries, promptly taking advantage of new technological developments can be crucial for remaining competitive and securing the organization's existence. Nowadays, a successful organization without IT is hard to imagine. From an individual's perspective, the usage of modern technologies (e.g., smartphones, tablets, or wearables) in private life has become similarly important. The technologies do not only offer new possibilities to communicate and interact with others, they also provide essential assistance in organizing everyday life. Against the background of extensive usage of IT in private and professional life, the amount of digitalized personal and organizational information is rapidly and incessantly rising. According to a recent report from IBM (2016), "[...] 90 percent of the data in the world today has been created in the last two years alone [...]" (p. 3). The International Data Corporation (IDC) predicts that the total amount of digital data annually created worldwide will increase from 4.4 zettabytes in 2013 to 44 zettabytes by 2020, that is an impressive number of 44,000,000,000,000 gigabytes newly created every year (IDC 2014a).

Because of the enormous data base emerging, private individuals and organizations using modern IT become attractive targets for attackers. This is also reflected in the disproportionate, increasing number of IT security incidents. At least since the Sony Picture Entertainment hack (e.g., BBC 2014), the Yahoo hack (e.g., Guardian 2016), the iCloud hack (e.g., Forbes 2014), or the Uber hack (e.g., Guardian 2017) — just to name a few prominent examples — the topic of IT security attracts high media attention and is highly discussed in research and society. The danger that arises from extensive IT usage is well recognized and,

accordingly, the global market for IT security products is constantly growing (Statista 2017a). However, although the members of our society should be actually aware of the importance of IT security in the digital age, both private individuals and organizations often refrain from adopting the necessary IT security measures. IDC stated that while 40 percent of the annually created data actually require a certain degree of data protection, less than 20 percent are respectively protected (IDC 2014a).

Considering the ongoing digitalization, it can be assumed that the number and variety of IT security threats that individuals and organizations are exposed to will continue to grow. IT experts assess IT developments like *Internet of Things* and *Cloud Computing* to be main drivers for change in IT security (Statista 2017b). It is predicted that, compared to 2015, the estimated annual cost for data breaches worldwide will increase almost four times to \$2.1 trillion by 2019 (Forbes 2016). Obviously, it is absolutely necessary to better prepare our society — both private individuals and organizations — for the growing danger resulting from the increasing number of IT security risks. To this end, useful recommendations and promising methods that encourage organizations as well as private individuals to actively protect their data from risks must be developed, tested, and improved.

From a theoretical point of view, it must be considered that IT security-related decisions of individuals within the private context and managers within the organizational context are made against the background of different environmental conditions. Therefore, the decisions are probably influenced by and based on different factors. Accordingly, existing studies in Information Systems (IS) research analyzing IT security perceptions and behaviors can be divided into two categories: studies conducted within the private context and studies conducted within the business context. Within the private context, many researchers investigated how individuals perceive risks that are associated with the usage of IT and how these risk perceptions influence their consequent behavior (e.g., Featherman and Pavlou 2003; Lee 2009; Liebermann and Stashevsky 2002). More specific, many studies are focused on analyzing privacy-related risk perceptions that arise from disclosing private information when using modern IT (e.g., Acquisti and Grossklags 2004; Krasnova et al. 2009; Shin 2010). For example, it is found that the perception of privacy risks can be the reason for an individual to refrain from using social networks, e-banking, or location-based services (e.g., Lee 2009; Smith et al. 2011; Zhou 2011). As such, these studies analyze how risks perceived by individuals influence their (amount of) IT usage. Studies focusing on how individuals decide to implement an IT security safeguard to stay safe while using IT in everyday life are rare.

The extant literature that focuses on individuals' adoption of IT security safeguards, such as anti-spyware software or backups (e.g., Boss et al. 2015; Liang and Xue 2010), mostly builds on quantitative data collected with questionnaires. As a consequence, the analyses and results are based on adoption intentions and behaviors as stated by the participants. Findings from psychological research that demonstrate that intentions do not always lead to appropriate behaviors or that stated behaviors do not necessarily match with actual behaviors (Sheeran 2002) are largely neglected. Moreover, none of the existing studies in the private context considers that females and males differ in their risk evaluations and protection behaviors in a wide variety of domains (e.g., Byrnes et al. 1999; Harris et al. 2006). For example, males are often found to be more likely to ride a motorcycle without a helmet or to abstain from using sunscreen (e.g., Byrnes et al. 1999; Harris et al. 2006; Johnson et al. 2004). Although having gender-mixed samples and despite inconsistencies among the findings, none of the existing studies analyzes the existence and role of gender differences when investigating risk perceptions and protective behaviors in the IT security domain.

Within the business context, the extant research predominantly pays attention to IT security perceptions and behaviors at the employee level. Employees are often considered to be the key factor for ensuring a high level of IT security within an organization (Bulgurcu et al. 2010). In particular, the compliance behavior of employees with an organization's IT security policies is often in focus (e.g., Boss et al. 2009; Bulgurcu et al. 2010; Pahnla et al. 2007; Siponen et al. 2010; Vance et al. 2012). In this context, employees' IT security awareness is identified to play a central role because it significantly influences the downstream assessments of perceived risks and, therefore, the consequent intentions and security-related behaviors (Bulgurcu et al. 2010). Based on that, several security education, training, and awareness (SETA) programs for increasing the IT security awareness at the employee level have been developed, analyzed, and tested (e.g., Doherty and Fulford 2006; Puhakainen and Siponen 2010; Siponen 2006; Siponen et al. 2010). Moreover, many studies investigated the role of managers in improving employees' security awareness and behaviors. As such, a top-down effect from the management level to the IT security behavior at the employee level is assumed (e.g., Kritzing and Smith 2008): Managerial actions toward IT security increase the IT security awareness at the employee level (e.g., Albrechtsen and Hovden 2010; Haeussinger and Kranz 2013; Spears and Barki 2010) and, therefore, enhance employees' IT security behaviors (e.g., Bulgurcu et al. 2010; Hu et al. 2012). However, while these studies clearly emphasize the crucial role of managers in ensuring a high level of IT security within an organization (e.g., Ashenden 2008; Sharma and Yetton 2007), IS research on IT security

from the perspective of managers is still rare. Consequently, IT security perceptions and coping behaviors at the management level are still far from being well understood and more research is needed.

## 1.2 Objectives and Research Questions

Overall, within the private and business context, prior research on IT security perceptions and behaviors leave many research questions unanswered. Considering the rapid evolution and the ever-increasing complexity of IT security risks, the need for further research on IT security perceptions and coping behaviors of private individuals and managers in organizations appears even more important. To address this, the overarching objective of this thesis is to advance our understanding about IT security perceptions and behaviors of private individuals and managers in organizations. In sum, this thesis includes four studies (one within the private context and three within the business context) — each addressing another research question. The results of the four studies were published in the proceedings of different reputable conferences, provide a basis for new research avenues, and come with numerous implications for private individuals as well as practitioners. In the following, a summary of the four research questions and the corresponding objectives are presented. In chapters 3 to 6 of this thesis, related research and identified research gaps will be presented in more detail.

Studies on IT security perceptions and behaviors within the private context often show inconsistencies in their findings. In psychological research, it is assumed that females' and males' appraisals of risks and behaviors are based on different cognitive processes because they are differently educated by society (Bem 1981). Even in times of gender equality, females and males are still somehow differently educated, especially when it comes to risk assessments. For example, parents might be more worried about letting their teenager walk home alone from a party in the middle of the night in the case of a girl. As such, females are still often considered to be somehow more vulnerable than males, which, in turn, influences the way females and males are educated when it comes to risk assessments and behaviors. As a consequence of different education, males and females can have different cognitive associations with certain types of information and, therefore, exhibit different behaviors (Bem 1981; Tamres et al. 2002). If females and males really differ in their risk perceptions and behaviors in the IT security domain, it is indispensable to understand these gender differences for formulating useful recommendations and for developing appropriate IT security safeguards. Therefore, the study presented in chapter 3 addresses the following research question (RQ):

*RQ 1: How do females and males differ in their IT security perceptions and protective behaviors?*

As mentioned in 1.1, previous research on IT security perceptions and behaviors within the organizational context is predominantly focused on the employee level. Up to now, only a few studies analyzed IT security perceptions and behaviors from the perspective of managers in organizations. Consequently, many research gaps exist that must be addressed in order to improve our understanding of managers' IT security perceptions and behaviors. Research regarding the following three aspects is especially rare: IT security awareness at the management level, managers' willingness to pay for IT security, and perceptual biases that distort managers' risk assessments.

While findings from studies at the employee level showed that IT security awareness significantly influences IT security perceptions and behaviors (e.g., Bulgurcu et al. 2010; D'Arcy et al. 2009; Goodhue and Straub 1991), only a few studies investigated the concept of IT security awareness at the top management level and its influence on the effectiveness of an organization's IT security management (e.g., Choi et al. 2008; Isomäki and Bilozerov 2012; Ng and Feng 2006). An organization's top management ultimately decides about resource allocations and thus, also largely determines an organization's investment decisions regarding IT security. Therefore, the IT security awareness of managers can be assumed to be at least of equal importance for ensuring a high level of IT security as the awareness of the organization's employees. In order to improve current knowledge about the concept of top managers' IT security awareness and its role in the organizational IT security management and to provide useful recommendations, the study presented in chapter 4 addresses the following research question:

*RQ 2: What is the role of top managers' IT security awareness in the organizational decision-making about IT security investments?*

There is also little knowledge about how much managers are willing to pay for implementing IT security safeguards in their organizations' IT systems and how their willingness to pay (WTP) is formed. Previous research on technology adoption shows that the perceived costs negatively influence adoption behaviors — in both the private context (e.g., Featherman and Pavlou 2003; Kim et al. 2007) and the business context (e.g., Kuan and Chau 2001; Saunders and Clark 1992). Furthermore, studies within the private context showed that the negative influence of perceived costs on an individual's adoption decision is also significant regarding the adoption of IT security safeguards (Boss et al. 2015; Liang and Xue 2010). A significant

effect of financial reasons on adoption decisions can also be expected in the business context but it is, however, not further analyzed until now and managers' WTP for IT security is far from being well understood. Therefore, the study presented in chapter 5 addresses the following research question:

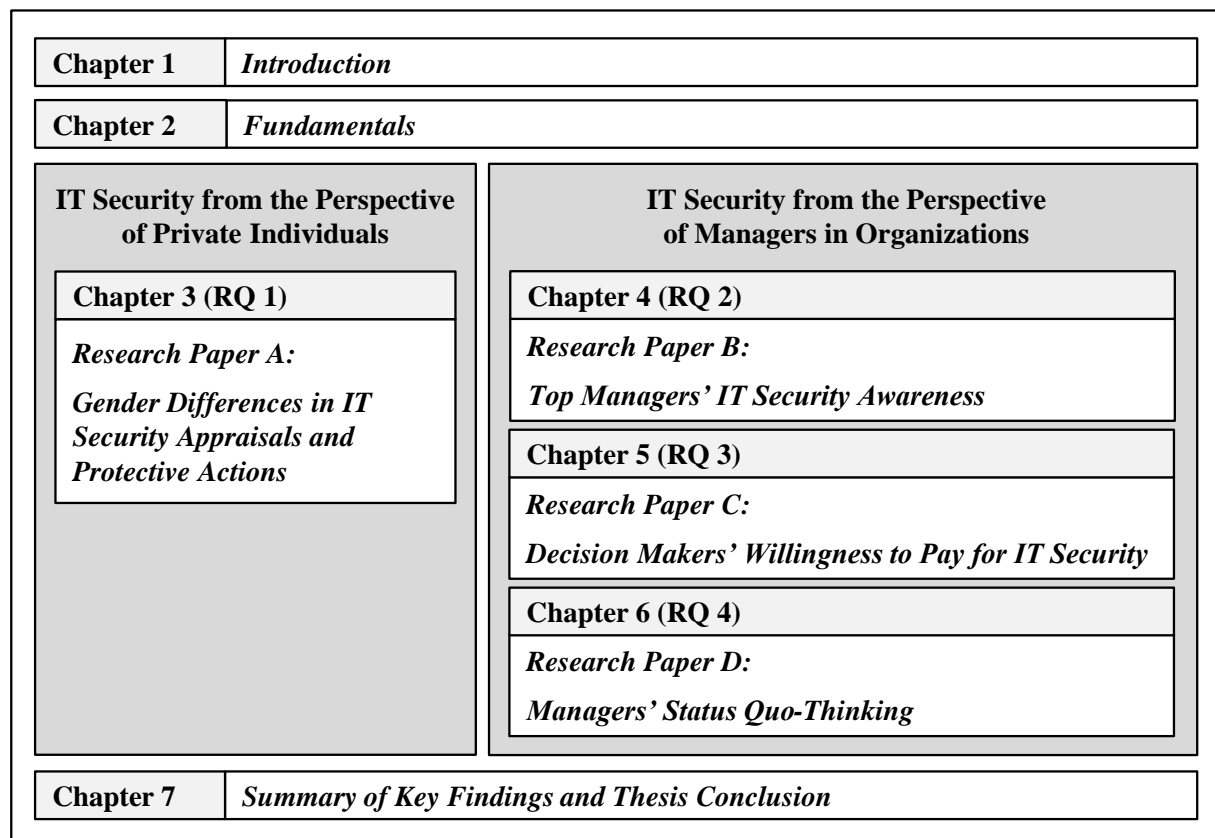
RQ 3: *How is managers' willingness to pay for IT security determined?*

From psychological research, it is known that individuals often tend to inadequately assess risks that they are exposed to, especially in uncertain situations. Various reasons for such a bias in risk assessments and their consequences were investigated (see e.g., Tversky and Kahneman 1975). In IS research, previous studies found that managers' IT security risk assessments are also subject to perceptual biases which can result in insecure behaviors (e.g., Loske et al. 2013; Rhee et al. 2012). For instance, Loske et al. (2013) and Rhee et al. (2012) analyzed the so-called *Unrealistic Optimism*, which is a bias in risk perception possibly arising when comparing the 'own vulnerability' to risks with the vulnerability of others during risk assessment. However, when analyzing managers' IT security-related decisions, not only the comparison of other organizations, but also the comparison of the current situation, might be relevant and thereby influence managers' risk assessments. For example, a manager might perceive a currently used IT system to be secure because the organization never experienced — or never recognized — an IT security incident due to its usage. However, the security risks of this system might be immense so that the implementation of a specific safeguard or a replacement of the system with a new, more secure one might actually be necessary. In this case, the manager uses the past experience as a reference point when assessing the currently present risk that may lead to an underestimation of the risk. In psychological research, the usage of reference points when assessing new technologies is called *Status Quo-Thinking* and can result in a *Status Quo Bias* (e.g., Kahneman et al. 1991; Samuelson and Zeckhauser 1988; Schweitzer 1995). This perceptual bias, which may lead to the insecure behavior of managers because of an inadequate evaluation of risks, is in the focus of the fourth research question in chapter 6:

RQ 4: *How does Status Quo-Thinking influence managers' decisions in adopting new IT systems?*

### 1.3 Structure of the Thesis

The thesis is organized into seven chapters (see Figure 1). Following this introductory chapter, the theoretical and methodological fundamentals are introduced in chapter 2. The core of this cumulative dissertation comprises four peer-reviewed and published research papers — each addressing one of the four research questions outlined hereinabove.<sup>1</sup> The first research paper focuses on IT security perceptions and behaviors from the perspective of private individuals and is presented in chapter 3. The other three research papers are based on studies that focus on the perspective of managers in organizations. These three papers within the business context are presented in chapter 4 to 6. Finally, the thesis concludes in chapter 7 with a summary of the key findings and implications.



**Figure 1: Structure of the Thesis**

In the following, the four research papers included in this thesis are listed and briefly summarized. The summaries as well as the research papers in chapters 3 to 6 are written from the first-person-plural point of view (i.e., we) in order to express that the four studies were conducted with co-authors and, therefore, they also reflect their opinions. The four research papers along with their respective publication outlets and publication dates are:

<sup>1</sup> To ensure a consistent layout throughout the thesis, the four published research papers in chapters 3 to 6 are presented in a slightly revised version from the original.



**Research paper A:** Sonnenschein, R., Loske, A., and Buxmann, P. 2016. “*Gender Differences in Mobile Users’ IT Security Appraisals and Protective Actions: Findings from a Mixed-Method Study.*” In: Proceedings of the 37<sup>th</sup> International Conference on Information Systems (ICIS), Dublin, Ireland. **VHB: A.**

**Research paper B:** Sonnenschein, R., Loske, A., and Buxmann, P. 2017. “*The Role of Top Managers’ IT Security Awareness in Organizational IT Security Management.*” In: Proceedings of the 38<sup>th</sup> International Conference on Information Systems (ICIS), Seoul, South Korea. **VHB: A.**

**Research paper C:** Sonnenschein, R., Loske, A., and Buxmann, P. 2016. “*Which IT Security Investments Will Pay Off for Suppliers? Using the Kano Model to Determine Customers’ Willingness to Pay.*” In: Proceedings of the 49<sup>th</sup> Annual Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii, USA. **VHB: C.**

**Research paper D:** Heidt, M., Sonnenschein, R., and Loske, A., 2017. “*Never Change A Running System? How Status Quo-Thinking Can Inhibit Software As A Service Adoption In Organizations.*” In: Proceedings of the 25<sup>th</sup> European Conference on Information Systems (ECIS), Guimarães, Portugal. **VHB: B, SIGSVC (Special Interest Group on Services in the AIS) Best Paper of the Year Award.**

**Research paper A** (chapter 3) draws on *Gender Schema Theory* (Bem 1981) and *Protection Motivation Theory* (Rogers 1975) and analyzes gender differences in IT security perceptions and behaviors of mobile users (RQ 1). By utilizing a two-step mixed-method research approach (step 1: survey, step 2: experiment and interviews), we collected data from 177 Android users (71 female and 106 male mobile users). Our results show that female and male mobile users’ security behaviors are based on different threat and coping appraisals. Moreover, while we found a significant relationship between protection intentions and the implementation of technical IT security safeguards in the female sample, we did not find one in the male sample. Overall, the results of this study show that gender differences in IT security perceptions and behaviors of private individuals exist and offer important implications for practice and future research.

Our study in **research paper B** (chapter 4) is focused on understanding the concept of top managers’ IT security awareness in the organizational IT security management (RQ 2). Based on a structured literature review and expert interviews, we developed and tested a conceptualization of top managers IT security awareness, including its role in the

organizational IT security management. In total, we identified seven factors that form two distinct dimensions of managerial IT security awareness (four factors in the individual dimension and three factors in the organizational dimension). We show that top managers' IT security awareness ultimately determines the scope for action (i.e., budget, human resources, and flexibility in decision-making) of the IT security specialists and thus, the IT security level of the organization. Furthermore, our results indicate that not only the awareness of top managers but also of managers at the department level is crucial for ensuring a high level of IT security. The proposed conceptualization will enable both future research and practitioners to improve our understanding of top managers' IT security awareness and its role in the organizational IT security management, and subsequently, to develop and improve interventions dedicated at increasing managers' IT security awareness and the effectiveness of an organization's IT security management.

By drawing on *Kano's Theory of Attractive Quality* (Kano et al. 1984), **research paper C** (chapter 5) analyzes how managers evaluate the available IT security safeguards and how this evaluation determines their willingness to pay (WTP) (RQ 3). Based on expert interviews and an empirical study within 84 managers from different organizations, we found that managers differently evaluate IT security safeguards and that this evaluation determines their willingness to pay. The results enable researchers and practitioners to better understand the different needs among various organizations as well as the associated willingness to pay of managers. Suppliers of IT security products can use the findings to improve their IT security strategies, which may provide both economic and competitive advantages.

**Research paper D** (chapter 6) is focused on *Status Quo-Thinking* of managers when deciding to adopt a new technology (RQ 4). Drawing on *Prospect Theory* (Kahneman and Tversky 1979) and *Status Quo Bias* research, we derived a research model that explicates the influence of the incumbent technology on the evaluation of benefits and risks of SaaS. Based on 123 data sets conducted with the help of a survey among different managers, we empirically tested our developed model and thereby demonstrated that managers' attitude toward a new technology is highly dependent on their assessments of the current systems and their experiences with the new technology. A lack of experience will increase the impact of the Status Quo on managers' assessments of a new technology and, therefore, probably result in an incorrect risk assessment that inhibits managers to adopt a potential advantageous technology, such as a new IT security safeguard.

## 2 Fundamentals

This chapter provides an overview of the fundamentals for the thesis.

### 2.1 IT Security Objectives

In general, IT security aims at protecting data and IT systems regarding their confidentiality, integrity, and availability (Blackwell 1998; Fried 1994). *Confidentiality* refers to the protection of data and IT systems from unauthorized access, *integrity* is protecting data and IT systems from unauthorized modification, and *availability* aims at ensuring that data and IT systems can be accessed by all authorized entities (Ma and Ratnasingam 2008). These three security objectives are also called the “golden security triangle” of CIA (confidentiality, integrity, and availability) (e.g., Shameli-Sendi et al. 2016) or “CIA triad” (e.g., Perrin 2008). Over time, researchers and practitioners introduced several other IT security objectives such as performance or non-repudiation (see e.g., Avižienis et al. 2004; Bedner and Ackermann 2010; Gouscos et al. 2003). For example, Ackermann et al. (2012) developed a conceptualization of IT security in the context of IT outsourcing and included performance, accountability, and maintainability aside confidentiality, integrity, and availability. However, these objectives are often context-dependent and can be subsumed under the CIA triad.

### 2.2 Risk Perception

For a reliable assessment of risks, a strong data base (e.g., long-term historical data) is needed. When the required data base is missing, risks are generally evaluated by people and, therefore, capture perceived risks that may differ from the actual risks (Slovic 1987). For example, when a study participant is asked to assess a risk they are exposed to, the risk measure represents their risk assessment and is a subjective judgment about the probability and potential damage of a negative event that does not necessarily correspond to the actual risk. Therefore, the risk-related decisions of individuals are generally based on perceived risks (Gigerenzer 2004) which may differ from the actual risks and, accordingly, lead to an incorrect risk assessment. Perceived risks are especially relevant in decision-making under uncertainty, discomfort and/or anxiety, and conflict (Bettman 1973).

In a wide area of domains, individuals have been found to be very incongruent in their risk perceptions (e.g., McKenna 1993; Perloff and Fetzner 1986; Weinstein 1982; Weinstein and Klein 1996). In the context of IT security, previous research showed the existence of phenomena like *Unrealistic Optimism* and *Illusion of Control* (Loske et al. 2013; Rhee et al. 2005; Rhee et al. 2012). The phenomenon of *Unrealistic Optimism* refers to an optimistic bias that results from comparing oneself with others when assessing risks (Weinstein (1980); see also *Theory of Social Comparison* (Festinger 1954)). As mentioned above, a reliable risk assessment requires a strong data base. When individuals do not have the relevant information for objective risk assessments, they regularly start comparing themselves to others that show similar characteristics (Wood 1989). Individuals are biologically prone to factors like self-enhancement, egocentric thinking, or representativeness heuristic, and perceiving own risks as lower than others' risks is gratifying (Shepperd et al. 2002). As a consequence, they tend to be unrealistically optimistic in their comparative risk assessments. Perceiving oneself at a lower risk versus comparable others relativizes the threat, lets the threat appear less harmful and, therefore, increases personal well-being (Wills 1981). *Illusion of Control* is an exaggeration of perceived controllability (Hoorens 1996; Langer 1975) and is closely related to *Unrealistic Optimism*. Specifically, perceived controllability is an individual's belief about how capable one is to achieve what is desired and prevent undesired events (Patrick et al. 1993) and it is found to influence an individual's risk perceptions. Similar to risk perception, individuals have been found to show a self-serving tendency when assessing control (Hoorens 1996; Langer 1975).

Perceived risks are known to have a strong influence on attitudes and intentions (Ajzen 1985; Smith 1992). Psychological research repeatedly demonstrated that perceived risks largely predict individuals' protection behaviors (e.g., Rogers 1975; Weinstein 1993; Witte 1992). Therefore, an underestimation of risks may result in not taking the necessary actions (e.g., implementing an IT security safeguard) and can have far-reaching consequences. Moreover, previous studies in IS research showed that perceived IT security risks can inhibit an individual to adopt a new technology like e-commerce or e-banking (e.g., Lee 2009; Liebermann and Stashevsky 2002; Luo et al. 2010).

Similar to the *Theory of Social Comparison*, the so-called *Prospect Theory* (Kahneman and Tversky 1979) considers that decisions under uncertainty (e.g., missing information) are not necessarily based on a rational weighing up of risks and benefits and their corresponding probability weights. It is argued that individuals' value functions are rather dependent on

reference points than on the actual final outcomes. When individuals are confronted with the decision to adopt a new technology, information or experience is often only limitedly available due to the degree of innovation. Therefore, an existing technology will serve as a reference point when assessing the new technology (e.g., Kahneman and Tversky 1979; Shoham and Fiegenbaum 2002). For example, when an individual sees an advertisement of a new bank, which claims to provide a more secure e-banking to their customers, the individual will probably use his or her current bank as a reference point because of missing experience with the newly advertised one. If the individual has never experienced a security incident in e-banking, the risk perceived to be associated with the current bank is automatically lower and the perceived risk of switching to the new one higher. However, the security level of the new bank may actually be higher. In this case, an incorrect assessment of IT security risks inhibits the individual from adopting a new, more secure technology.

### **2.3 Research Design and Methods**

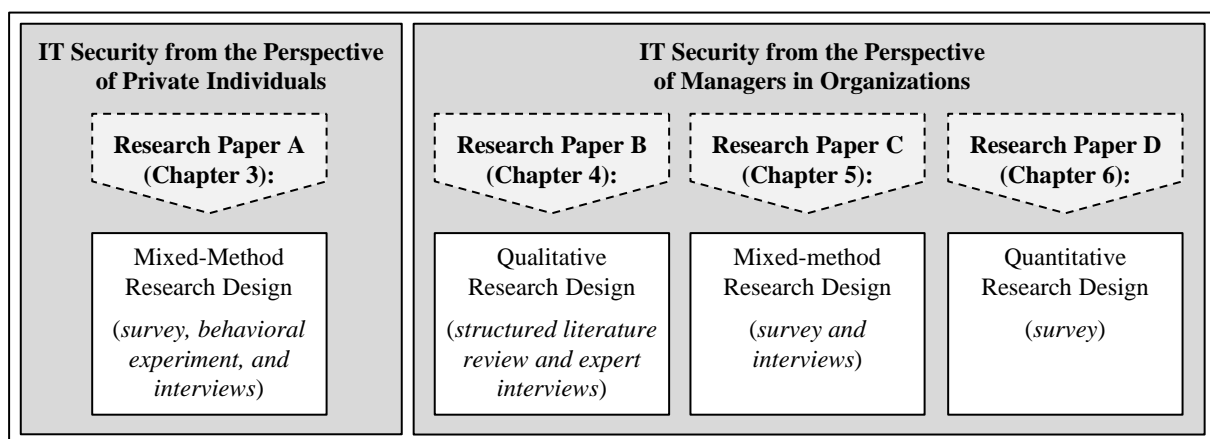
This section provides an overview and discusses the methods selected for the research designs within the four research papers in this thesis (chapters 3 to 6).

A large amount of different research methods exist that have been successfully applied by previous research in different domains. These methods can be distinguished in many different ways, whereas the categorization in quantitative and qualitative research methods is the most common one (Myers 1997). The main differences between these two categories are given by the data sample, data collection, and data analysis. Quantitative research methods have their origin in the natural sciences and were used for studying natural phenomena (Myers 1997). As such, quantitative studies generally aim at quantifying data in order to generalize statistical results from a sample to an entire population of interest. Contrarily, qualitative methods originally stem from the social sciences (Myers 1997) and are assumed to be particularly suitable for gaining an in-depth understanding of motivations and behavioral phenomena. While qualitative research methods are typically exploratory in nature, quantitative methods are generally highly structured and rather explanatory. For example, quantitative research methods include surveys, numerical methods, laboratory experiments, and formal approaches (Myers 1997) while case studies, action design, or grounded theory studies belong to the category of qualitative methods (Creswell 2014; Myers 1997). The two categories of research methods have different benefits and shortcomings. For example, while qualitative methods can support researchers in gaining well-grounded descriptions and explanations of a “real-

world phenomena”, quantitative methods come along with benefits like careful measurement, experimental control, generalizable samples, and statistical tools (Miles and Huberman 1994).

Both categories are well-accepted in the IS discipline and need not be viewed as incompatible since they can also be combined. A combination of multiple qualitative and quantitative research methods within a single study is called “mixed-method research” (Creswell 2014; Venkatesh et al. 2013). Previous work strongly encourages IS researchers to conduct more mixed-method studies for several reasons (Mingers 2001; Venkatesh et al. 2013). For example, mixed-method studies can provide complementary views on the same phenomena or relationship and they can be helpful in gaining a complete picture of a phenomenon or in compensating for the disadvantages of one method. A list of different purposes to use mixed-method approaches can be found in Venkatesh et al. (2013).

The studies within the present thesis include quantitative, qualitative, and mixed-method research designs. An overview of the different research designs used in the respective studies is shown in Figure 2.



**Figure 2: Overview of Research Design and Methods in the Thesis**

For analyzing gender differences in mobile users’ IT security perceptions and behaviors (research paper A), a two-step mixed-method approach under laboratory conditions is chosen in order to gain a holistic understanding (Venkatesh et al. 2013). In the first step, the participants were asked to complete a survey, whereas the second step comprised a behavioral experiment and qualitative interviews. The quantitative and qualitative data were concurrently collected and integrated for data analysis (Creswell 2014; Venkatesh et al. 2013). By applying a mixed-method design, we were not only able to measure the perceptions and stated intentions of the participants but also their actual behaviors.

In research paper B (chapter 4), a structured literature review and qualitative expert interviews were conducted. The structured literature review serves as basis for developing a conceptualization of top managers' IT security awareness (Webster and Watson 2002). Then, the developed conceptualization is evaluated by conducting qualitative expert interviews. The interviews were conducted due to several reasons: to confirm and expand the proposed conceptualization, to gain complementary views on the concept, and to ensure a complete picture of the phenomenon.

The investigation of managers' willingness to pay in research paper C (chapter 5) also applies a mixed-method research design. Due to its explorative nature, the study starts with qualitative expert interviews that serve as basis for preparing the survey for a quantitative study. By combining the two research methods, the hypothesized theoretical relationships can be tested.

Finally, research paper D (section 6) employs a quantitative method to analyze managers' Status Quo-Thinking. Specifically, a survey is chosen for data collection because this quantitative research method is appropriate for ensuring a careful measurement and allows generalizing results to a population of interest.

### 3 Research Paper A: Gender Differences in IT Security Appraisals and Protective Actions

**Title:** Gender Differences in Mobile Users' IT Security Appraisals and Protective Actions: Findings from a Mixed-Method Study

**Authors:** Sonnenschein, Rabea  
Loske, André  
Buxmann, Peter

**Published in:** Proceedings of the 37<sup>th</sup> International Conference on Information Systems (ICIS), Dublin, Ireland 2016

#### Abstract

*Recent reports show that mobile users often refrain from taking the necessary precautionary actions to protect their mobile devices from IT security threats. To improve users' protective behavior, it is necessary to have a better understanding of the downstream beliefs and attitudes. Although previous IS research has intensively investigated protection behavior in the IT context, findings from psychological studies that people's threat and coping appraisals are gender-specific are largely neglected. Drawing on Gender Schema Theory and Protection Motivation Theory, the present study analyzes gender differences in the formation of mobile users' intentions to take precautionary actions and their consequent coping behavior. Utilizing a two-step mixed-method research approach (survey, experiment, and interviews) and drawing data from 177 Android users, we show that female and male mobile users' problem-focused coping behaviors are based on different threat and coping appraisals. These findings have significant implications both for future research and for practitioners.*

**Keywords:** Gender Differences, Gender Schema Theory, Protection Motivation Theory, Threat Appraisal, Coping Appraisal, Mobile Security.



### 3.1 Introduction

Mobile devices presently constitute an inherent part of our everyday lives. The rapid increase in mobile device usage has led to a shift in security breaches from traditional PCs to tablets and smartphones (Gartner 2014). In particular, mobile devices are known to be repositories for large amounts of personal data, such as contact information, e-mails, calendars, and profiles (Guardian 2015); thus, gaining access to a person's smartphone can enable an attacker to produce a large amount of damage. Recent studies report that 5.2 million smartphones are lost or stolen in the US every year and that over 25% of all mobile devices encounter a network attack each month (Skycure 2015). Moreover, it has been found that nearly one out of four (24.7%) mobile apps include at least one high-risk security flaw (NowSecure 2016). Although the potentially far-reaching consequences (e.g., financial, reputational, and psychological damage) of mobile IT security incidents are well recognized in today's society, security reports have found that users often refrain from actively coping with existing mobile threats (i.e., they do not take the necessary precautionary actions, such as installation of safeguarding measures) (AVAST 2014). In order to address this insufficient coping behavior, it is essential to understand how mobile users decide to actively cope with mobile IT security threats (i.e., to adopt safeguarding measures), including which factors this decision is based on.

Drawing on psychological research, studies on IT security behaviors postulate that individuals' protection intentions are fundamentally based on two cognitive processes: a threat appraisal (i.e., evaluation of the perceived IT security threat) and a coping appraisal (i.e., evaluation of available actions for coping with the perceived IT security threat) (Floyd et al. 2000; Fry and Prentice-Dunn 2005; Milne et al. 2002). Although several studies have analyzed the coping behavior of users in the IT context (e.g., Johnston and Warkentin 2010; Lee et al. 2008; Liang and Xue 2010), the results often exhibit inconsistencies regarding which factors significantly influence users' coping decisions. Moreover, despite having gender-mixed samples, existing studies largely neglect the finding from psychological research that females and males often differ in their cognitive appraisals of threat and consequent coping actions. In particular, psychological research has argued that females' and males' appraisals are based on different cognitive processes because society educates them differently (Bem 1981). For example, it is commonly believed that males are more likely to confront a problem head-on, while females exhibit more emotional responses to problems (Tamres et al. 2002). The different ways in which females and males are expected to cope with problems in turn influence how they are educated when they are children (Tamres et al.

2002) (e.g., boys are less likely than girls to receive their parents' understanding when they exhibit emotional responses to problems). As a consequence of their gender-specific education as children, females and males have different cognitive associations with certain types of information and thus exhibit different behaviors (Bem 1981). Considering the technological nature of IT security, which historically has tended to be seen as a more masculine discipline (Trauth et al. 2010), similar gender differences in cognitive appraisal processes and consequent coping behaviors are likely to influence coping actions in the IT security context. For example, males are generally believed to be more "into" technology than females, and males are therefore more encouraged in the course of their education to be action oriented regarding technology use (Tamres et al. 2002). As a result, females and males will have different cognitive associations with IT security-related information and will therefore base their decisions to cope with IT security threats on different cognitive processes. If females and males differ in their IT security appraisals (threat and coping appraisals), it is essential to understand these differences in order to effectively increase users' intentions to actively protect their devices and consequently increase the IT security level of mobile users, organizations, and in turn, society as a whole. Thus, this study addresses the following research question: *How do female and male mobile users differ in their IT security appraisals (threat and coping appraisals) and coping actions?*

In IS research, the role of gender has been the focus of several studies in different contexts. These studies can be roughly divided into two broad categories: studies that focus on gender differences in the IS workforce and studies that focus on gender differences in IT adoption and IT use (Trauth 2013). However, research on gender differences in the IT security context is rare. As such, the underlying cognitive processes — IT security threat and coping appraisals — are far from well understood. While a few studies analyze gender differences in IT security policy compliance behavior at the organizational level (Bansal et al. 2016; Bansal and Shin 2016), there is little research on gender differences in security appraisals and coping behavior at the individual level of analysis. Thus, we answer the call of Trauth (2013) to conduct more studies on gender differences in IS research since gender is a fundamental characteristic of users and thus is likely to have a substantial impact on individuals' IT security behavior.

Drawing on Protection Motivation Theory (PMT) and Gender Schema Theory, we derive a research model of mobile users' IT security behavior. Specifically, we apply Gender Schema Theory to analyze the role of gender in the threat and coping appraisals and consequent

coping behavior of mobile users, as suggested by PMT. In order to empirically test our theoretical model, we chose a two-step mixed-method research approach under laboratory conditions. This enabled us not only to analyze gender differences regarding self-stated appraisals and protection intentions but also to observe mobile users' actual coping behavior. In the first step, participants completed a survey regarding their IT security appraisals (threat and coping appraisals) and their intentions regarding protection behavior (coping actions). In the second step, we conducted a behavioral experiment in order to observe the participants' actual coping actions. Afterwards, we requested personal interviews with the participants. The qualitative data from the interviews enabled us to better understand how they made coping decisions, that is, the reasons for their IT-security-related decision making and, specifically, their previous coping actions within our study.

The findings of this paper have several important theoretical and practical implications. The study extends our knowledge about individuals' IT security behavior by examining how the gender of mobile users influences their cognitive IT security appraisals. Specifically, we found that female and male mobile users differ in their threat and coping appraisals and that their intentions to actively protect their mobile devices are influenced differently by these differences in their cognitive IT security-related perceptions. As this finding provides an opportunity to better explicate mobile users' IT security behaviors, it is relevant not only for future research but also for practitioners. Mobile IT security providers can learn that they should consider the differences between females and males regarding security appraisals and coping behaviors when designing their marketing campaigns, in order to effectively emphasize the need for protective IT security measures. Suppliers of IT security training and organizations faced with paradigms like Bring Your Own Device can also benefit from the results of our study. When developing security workshops and training, they need to educate and train females and males differently regarding how to handle IT security issues.

## **3.2 Theoretical Background and Hypothesis Development**

### *3.2.1 Protection Motivation Theory*

PMT (Rogers 1975) explains how individuals become motivated to cope with threats. PMT postulates that individuals' protection motivation is shaped by two key processes: a threat appraisal and a coping appraisal (Floyd et al. 2000; Fry and Prentice-Dunn 2005; Milne et al. 2002). The theory has been adapted to the IT security context by many researchers in different settings (e.g., Herath and Rao 2009b; Johnston and Warkentin 2010; Lee et al. 2008; Lee and

Larsen 2009; Liang and Xue 2010). For example, in the organizational context, PMT has been used to explain employees' security behavior (Workman et al. 2008) and information security policy compliance (Herath and Rao 2009b; Vance et al. 2012), and in the private context, it has been used to analyze home users' security behavior (Anderson and Agarwal 2010) and adoption of anti-spyware software (Johnston and Warkentin 2010). Overall, it is assumed that when individuals perceive an IT security threat to be present, they will start to assess the threat (threat appraisal) and will subsequently evaluate available behaviors to cope with the threat (coping appraisal) (Liang and Xue 2010).

In general, the threat appraisal is determined by an evaluation of the severity and the susceptibility of a threat. Severity refers to the damage that can be caused by the potential consequences of a security breach, and susceptibility is the perceived likelihood that one will become subject to the threat (Prentice-Dunn and Rogers 1986). Accordingly, *perceived severity* in the context of mobile IT security is defined as the extent to which an individual perceives that the negative consequences that can be caused by IT security incidents are severe for his or her mobile IT device. *Perceived susceptibility* is an individual's perceived subjective probability that IT security incidents will negatively affect his or her mobile IT device (Johnston and Warkentin 2010; Liang and Xue 2010). Previous IS research assumes that perceived severity and perceived susceptibility do not directly influence protection motivation but will first result in a risk evaluation to determine the perceived security threat (Ng et al. 2009; Woon et al. 2005; Workman et al. 2008). The *perceived threat* is defined as the extent to which an individual perceives the mobile IT security threat as dangerous or harmful (Liang and Xue 2010). In the context of IT security, a mobile user may perceive an attack on his/her mobile banking account to be associated with a large amount of (financial) damage (severity) but as very unlikely to happen (susceptibility). In contrast, losing the mobile device may also be associated with a large amount of damage (e.g., monetary loss with respect to the mobile device and reputational damage with respect to private pictures) but perceived as much more likely to happen and thus will be evaluated as a higher threat.

In their coping appraisal, people determine the avoidability of a perceived IT security threat by considering two efficacy-related factors: the perceived effectiveness of a safeguard action and their perceived self-efficacy regarding implementation of safeguards (e.g., Johnston and Warkentin 2010; Liang and Xue 2009; Liang and Xue 2010). *Perceived effectiveness* is defined as an individual's subjective assessment of how effective a safeguard action is for avoiding IT security incidents (Johnston and Warkentin 2010; Liang and Xue 2010).

*Perceived self-efficacy* is defined as an individual's judgement of his or her personal skills, experience, knowledge, or competency regarding implementing safeguard actions against IT security threats (Compeau and Higgins 1995). Thus, the assessed effectiveness is determined by the perceived risk reduction that is achievable through implementation of the respective IT security safeguard, whereas the perceived self-efficacy is primarily determined by how confident people feel about implementing the IT security safeguard in order to cope with the perceived threat (Liang and Xue 2010).

Accordingly, mobile users' *protection intention* is defined as their stated behavioral intention to actively cope with mobile IT security threats in order to protect their mobile devices (Ajzen 1991; Davis 1989; Liang and Xue 2009). The protection intention that results from a rational weighing up of the individuals' threat and coping appraisals ultimately predicts the coping behavior. Individuals' actual protective behavior comprises their actual *coping actions* that are in line with their behavioral intention, e.g., the implementation of an IT security app.

### 3.2.2 Gender Schema Theory

Several theories have been used to analyze and explain differences in the perceptions and behaviors of females and males. Overall, these theories can be classified into two broad categories: theories that emphasize psychological and/or sociostructural determinants of gender differences (e.g., Social Role Theory) (Eagly and Wood 1991; Franke et al. 1997), and theories that emphasize biological differences (e.g., Evolutionary Theory) (Buss 1988).

Gender Schema Theory (Bem 1981) belongs to the first category and postulates that females and males differ in their cognitive information processing due to different socially construed cognitive structures that determine and direct their perceptions (see also Venkatesh and Morris 2000). Gender Schema Theory argues that societies allocate gender-specific roles to males and females and that these are anticipated in the societies' socialization of children. In particular, children are taught during their childhood what it means to be a woman or a man and how to behave consistently with this gender schema. Due to this different socialization and education, females and males learn "to process information in terms of an evolving schema" (Bem 1981, p. 355) and thus develop gender-linked associations with information. As a consequence, females and males process information in decision-making situations based on different cognitive processes (Venkatesh and Morris 2000).

Previous research has shown that Gender Schema Theory is useful for analyzing gender-specific differences in the cognitive appraisals that lead to decision making in the context of

technology adoption (e.g., Venkatesh and Morris 2000). Therefore, we apply Gender Schema Theory to the theoretical underpinnings assumed by PMT in order to analyze the role of gender differences in mobile users' threat and coping appraisals as well as their consequent coping behavior.

### *3.2.3 Gender Differences in Appraisals and Coping Behaviors of Mobile Users*

According to PMT, coping behavior in the context of IT security is based on two cognitive appraisals: the appraisal of the threat (threat appraisal) and the appraisal of the resources that are available to address the threat (coping appraisal). From a Gender Schema Theory perspective, these two cognitive appraisals might be influenced by gender due to gender-specific cognitive information processing. This assumption is also in line with previous research that has found that males and females differ in their threat appraisals and coping behaviors in other contexts (e.g., Dias et al. 2010; Lengua et al. 1999; Ptacek et al. 1992). Females are often seen as the more risk-averse gender (e.g., Byrnes et al. 1999; Harris et al. 2006), while males are commonly viewed as being more likely to engage in risk behavior such as riding a motorcycle without a helmet or not using sunscreen (e.g., Byrnes et al. 1999; Harris et al. 2006; Johnson et al. 2004). According to Gender Schema Theory, these beliefs about females' and males' expected behavior lead to a socialization of boys and girls according to which risk behavior is rather "masculine" (Byrnes et al. 1999; Wilson and Daly 1985). In particular, females and males are educated differently regarding the way they appraise threats, and this might also impact their threat appraisal in the context of mobile IT security threats. A coping appraisal is based on an appraisal of one's resources for addressing a threat (Tamres et al. 2002), and psychological research has therefore found that males evaluate information in the context of coping appraisals differently from their female peers, who are socialized to be more self-critical (Prentice and Carranza 2002). Considering that males are often found to show higher levels of self-confidence than females in the context of technology (Lenney 1977) and that they can be understood as the gender that is socialized to be self-confident, information processing within the coping appraisal might also be influenced by mobile users' gender. In sum, using the theoretical underpinnings of Gender Schema Theory to analyze the causal relationships that are assumed by PMT leads to the conclusion that mobile users' threat and coping appraisals — which ultimately influence users' intentions to actively cope with mobile IT security threats — are gender-specific because the underlying schematic processes are socially construed.

### 3.2.3.1 Gender Differences in Threat Appraisals

In line with previous research in the IT security context (Liang and Xue 2009), we assume that in a threat appraisal, both perceived severity and perceived susceptibility positively influence mobile users' perception of the security threat to their mobile devices. From a Gender Schema Theory perspective, it can be argued that female and male mobile users may differ in their threat appraisals because they are socialized to cope differently with threats. Females are generally seen as the more emotion-focused individuals, and psychological research shows that females experience emotion more intensively than males (Fujita et al. 1991). As a consequence, females may base their threat perception primarily on their assessments of how emotionally upset or harmed they would be if the respective risk were to occur (Harris et al. 2006) and largely neglect considering the probability of the risk. In contrast, males are often seen as more problem-oriented and as applying more rational decision making (Pearlin and Schooler 1978; Stone and Neale 1984). Males are encouraged during childhood to confront problems head-on and objectively appraise situations rather than exhibiting emotional responses. Accordingly, it can be expected that male mobile users are more likely to be rational and include both perceived severity and perceived susceptibility in their evaluation of a perceived mobile IT security threat. Thus, it can be assumed that females base their threat evaluation primarily on perceived severity, while males' risk evaluations will be more rational and therefore influenced by both perceived severity and perceived susceptibility. This assumption of a weaker influence of perceived susceptibility on perceived threat within females is also in line with the findings of Levy and Baron (2005), who found that females are less sensitive to risk susceptibility and therefore base their risk perceptions primarily on perceived severity (see also Gal 1996). In contrast, males' threat perceptions have been found to be sensitive to both perceived susceptibility and perceived severity. Hence, in line with PMT and previous research on gender differences, we hypothesize:

***H1a:*** *Perceived severity will have an equal positive impact on the perceived IT security threat for male and female mobile users.*

***H1b:*** *Perceived susceptibility will have a stronger positive impact on the perceived IT security threat for male mobile users than for female mobile users.*

Previous research has conclusively shown that when a mobile user perceives a security threat to be relevant, she or he will have a stronger intention to cope with this risk (e.g., Liang and Xue 2009; Liang and Xue 2010). In general, males have been found to be more likely to engage in risk behavior (e.g., Byrnes et al. 1999; Hersch 1996), while females have been

found to be more likely to avoid risky situations (e.g., Byrnes et al. 1999; Harris et al. 2006). Considering that females are more likely to avoid risky behaviors and are often found to be more risk averse than males, females can be expected to be more sensitive to environmental risks than males. This is also in line with Evolutionary Theory, which argues that females have a greater tendency to avoid risks due to evolutionary reasons (Harris et al. 2006). Historically, females had to take care of their offspring and protect them from environmental risks, while males had to leave their safe homes to hunt. Thus, it can be assumed that the positive effect of a perceived mobile IT security threat on users' protection intention (e.g., installing a security app to reduce the perceived threat) will be stronger for female mobile users than for male mobile users. Thus, we hypothesize:

***H1c:*** *The perceived IT security threat will have a stronger positive impact on protection intentions for female mobile users than for male mobile users.*

### 3.2.3.2 Gender Differences in Coping Appraisals

Regarding the coping appraisal, PMT generally assumes that the perceived effectiveness (i.e., the perceived risk reduction) associated with a protective action has a positive effect on the protection intention (e.g., Liang and Xue 2009; Liang and Xue 2010). Considering Gender Schema Theory, this cognitive process might be also influenced by gender-specific cognitive associations. Males have been observed to be more task oriented than females in several contexts (e.g., Minton and Schneider 1985; Venkatesh et al. 2003). They learn in early childhood that males have to confront problems head-on and that males are more talented in technology use than females. Thus, the effectiveness of a certain coping behavior — especially in the context of IT — can be expected to have a stronger influence on decision making regarding coping behavior for males than for females. This assumption is also in line with the theoretical underpinnings of Social Role Theory (Eagly and Wood 1991; Franke et al. 1997) and findings from previous IS research (Minton and Schneider 1985; Venkatesh et al. 2003). According to Social Role Theory, males, in contrast to females, typically find their work role more important than their family role (Barnett and Marshall 1991). Due to these gender-specific roles that are manifested in society, males are expected to be more motivated by achievement needs (e.g., effectively coping with threats) than females are (Hoffman 1972). Moreover, previous IS research on IT adoption has found that when a technology is perceived to be effective, this will have a stronger positive effect for male users' intentions than for female users' intentions (Venkatesh et al. 2003). In line with previous research, we therefore hypothesize:



***H2a:*** *Perceived effectiveness will have a stronger positive impact on protection intentions for male mobile users than for female mobile users.*

Besides the effect of perceived effectiveness on protection intentions, PMT also postulates that individuals' perceived self-efficacy positively influences their protection intentions in their coping appraisals. From the Gender Schema Theory perspective, we need to consider that males have been found to be more self-confident than females in their technology-related skills (Li and Kirkup 2007). Compared to females, males tend to be less anxious about technology use (Bozionelos 1996). These differences between males and females may be rooted in the different ways that society educates males and females. While females are thought to be more anxious and less talented in technology use, males learn that their gender is known to be technically oriented. As a result, females' perceived self-efficacy is subject to higher levels of uncertainty, which in turn may weaken a positive impact of their perceived self-efficacy on their protection intentions. Gender differences in the relationship between self-efficacy and intentions have also been found by previous IS research, e.g., in the context of accepting the mobile internet (Wang and Hsu 2010). Accordingly, self-efficacy can be expected to have a stronger positive impact on the protection intention for male mobile users than for female mobile users. We hypothesize:

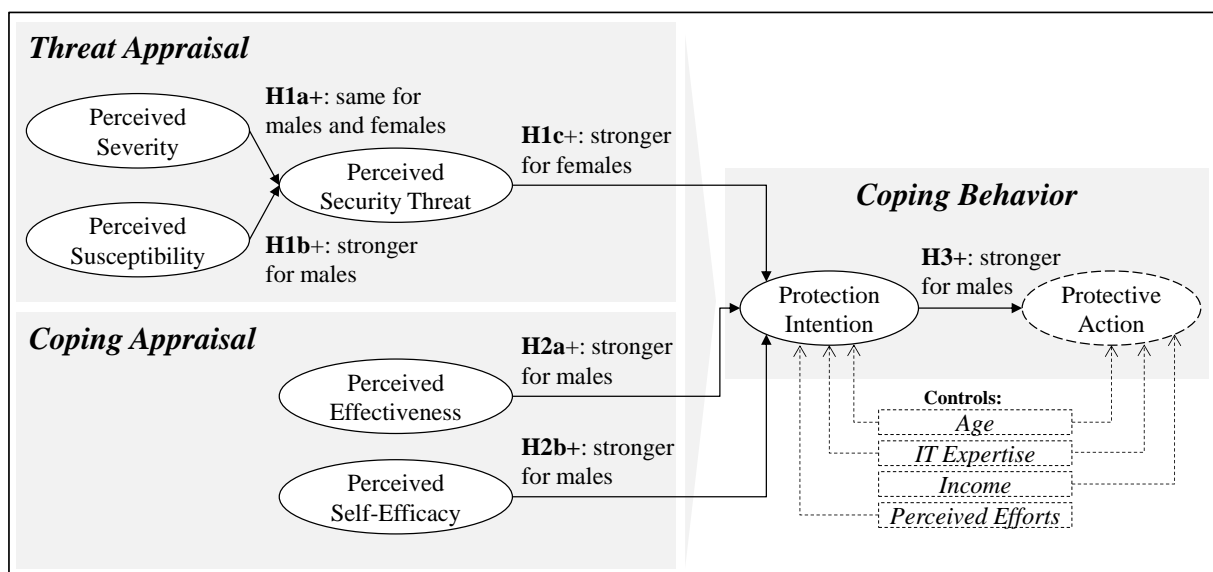
***H2b:*** *Perceived self-efficacy will have a stronger positive impact on protection intentions for male mobile users than for female mobile users.*

PMT assumes that individuals' intentions to perform actions directly influence their actual behavior. However, with regard to coping behaviors, it is commonly assumed that females and males differ in their choice of coping strategies. Specifically, research often assumes that males are more likely to apply problem-focused coping strategies (i.e., behavior that aims to alter a threat by actively changing the environment), while females tend to apply more emotion-focused coping strategies (i.e., behavior that aims to alter the emotional response to a threat without actually changing the environment) (Lazarus and Folkman 1984). A major reason for gender differences in coping behaviors is provided by the so-called socialization hypothesis (Ptacek et al. 1992). In line with Gender Schema Theory, it is argued that females and males exhibit different coping behaviors because they are socialized to deal differently with stressful and risky situations. Accordingly, males are generally thought to be more likely to confront problems head-on (Tamres et al. 2002), which in turn strengthens the relationship between their protection intentions and active coping behavior (e.g., implementing an IT security safeguard on a mobile device), which is a form of problem-focused coping (Tamres

et al. 2002). In contrast, female mobile users' protection intentions are expected to have a weaker impact on problem-focused coping, because they are socialized to deal with problems more emotionally and to be less action-oriented than males (Tamres et al. 2002). While a large stream of research has found that females and males differ in their coping behaviors in various contexts and situations, the findings of these studies are often inconsistent. For example, in certain situations (e.g., in coping with relationship stressors), males are found to apply more emotion-focused coping strategies (Tamres et al. 2002). Since problem-focused coping strategies in the context of mobile IT security require appraising technology-related threats and coping options as well as performing technology-related actions, we follow the widespread understanding of males as being the more problem-focused gender. Therefore, we hypothesize:

**H3:** *Protection intentions will have a stronger positive impact on protective actions for male mobile users than for female mobile users.*

The research model is shown in Figure 3.



**Figure 3: Research Model (Research Paper A)**

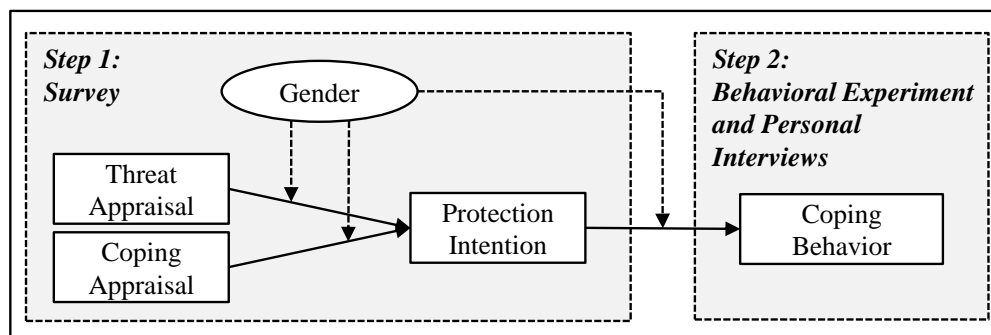
### 3.3 Research Methodology

#### 3.3.1 Research Approach

Most of the studies in IS research that examine individuals' protective behavior assume that an individual's intention to cope with a risk ultimately predicts his or her coping behavior, but they do not measure and analyze individuals' actual behavior. Hence, a common criticism is that most studies on security behaviors are restricted to the measurement of self-reported data

and do not analyze actual behavior (e.g., Boss et al. 2015; Vance et al. 2014). As a consequence, we are still far from understanding the actual IT security behavior of individuals (Boss et al. 2015). To address this issue, we chose a two-step mixed-method approach (see Figure 4) that includes a survey to gather quantitative data and a behavioral experiment and interviews to observe participants' actual coping behaviors.

In the first step, we used the survey to gather quantitative data about mobile users' threat and coping appraisals as well as their intentions regarding protective actions. We used the behavioral experiment and personal interviews in the second step to evaluate mobile users' actual coping behavior in terms of problem-focused coping actions such as actively implementing technical security measures (e.g., a security app) on their mobile devices.



**Figure 4: Research Approach (Research Paper A)**

We chose to conduct our study based on Android users because this is the most widely used mobile operating system and is often seen as the most vulnerable one. For example, Kaspersky (2014) reported that 99% of all mobile malware is designed to target the Android platform. Kaspersky (2014) argues that Android is especially attractive to attackers because of the open nature of the Android operating system and its market share of over 70%. We focused our study on users of one specific operating system to ensure comparable environmental conditions, such as IT security threats grounded on system-specific characteristics.

### 3.3.1.1 Step 1: Survey Development

We established construct validity by adapting items from previous research. We pre-validated our measurement model, the behavioral experiment, and the interviews in a pre-study. First, the survey was evaluated and revised by eight IS researchers. Next, we conducted the study under laboratory conditions with eight mobile users. This pre-test resulted in small changes to the structure and wording of the survey. The final items and scales that were used are presented in Table 1.

**Table 1: Items Used in the Quantitative Study**

<b>Construct (Sources)</b>	<b>Items / Scales</b>
<i>Perceived susceptibility</i> (Johnston and Warkentin 2010; Witte 1996)	My smartphone is at risk of being negatively affected by IT security incidents. (Susc1) It is likely that IT security incidents will negatively affect my smartphone. (Susc2) It is possible that IT security incidents will negatively affect my smartphone. (Susc3) (1 = <i>strongly disagree</i> – 7 = <i>strongly agree</i> )
<i>Perceived severity</i> (Herath and Rao 2009b; Johnston and Warkentin 2010; Witte 1996)	If there is an IT security incident on my smartphone, it will be severe. (Sev1) If there is an IT security incident on my smartphone, it will be serious. (Sev2) I believe that information stored on my smartphone is vulnerable to IT security incidents. (Sev3) (1 = <i>strongly disagree</i> – 7 = <i>strongly agree</i> )
<i>Perceived IT security threat</i> (Liang and Xue 2010)	IT security incidents that can happen on my smartphone pose a threat to me. (Risk1) IT security incidents are a danger to my smartphone. (Risk2) It will be dreadful if my smartphone is affected by an IT security incident. (Risk3) (1 = <i>strongly disagree</i> – 7 = <i>strongly agree</i> )
<i>Perceived effectiveness</i> (Johnston and Warkentin 2010; Witte 1996)	Use of a security app is especially effective for protecting my smartphone. (Effective1) Use of a security safeguard measure would increase my level of protection for my smartphone. (Effective2) (1 = <i>strongly disagree</i> – 7 = <i>strongly agree</i> )
<i>Perceived self-efficacy</i> (Bulgurcu et al. 2010; Compeau and Higgins 1995)	I can successfully choose and undertake mobile safeguard actions even if there is no one around to tell me what to do. (Self-eff1) I can successfully choose and undertake mobile safeguard actions if I have enough time to complete the job. (Self-eff2) I can successfully choose and undertake mobile safeguard actions since I have already carried out similar actions. (Self-eff3) (1 = <i>not at all confident</i> – 10 = <i>totally confident</i> )
<i>Protection intention</i> (Bulgurcu et al. 2010; Davis 1989; Fishbein and Ajzen 1975)	I intend to carry out all necessary safeguard actions to protect my smartphone against IT security incidents. (Int1) I plan to carry out all necessary safeguard actions to protect my smartphone against IT security incidents. (Int2) I intend to protect all the data stored on my smartphone and all apps

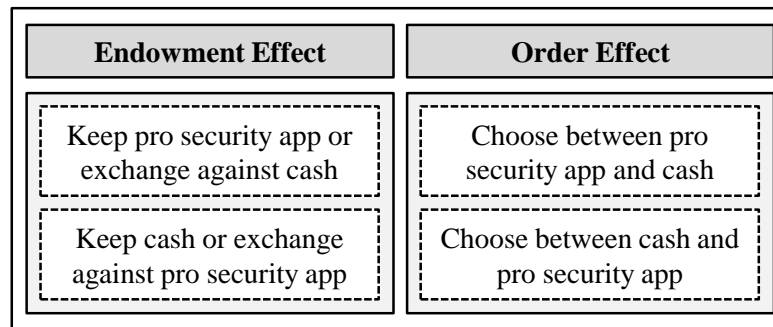
	operating on my smartphone by undertaking corresponding safeguard actions. (Int3) (1 = <i>strongly disagree</i> – 7 = <i>strongly agree</i> )
<i>Perceived effort</i> * (Bulgurcu et al. 2010; Liang and Xue 2010)	Undertaking safeguard actions to protect my smartphone against IT security risks is time consuming for me. (Effort1) Undertaking safeguard actions to protect my smartphone against IT security risks is burdensome for me. (Effort2) Choosing the right security app and using it is too much trouble. (Effort3) (1 = <i>strongly disagree</i> – 7 = <i>strongly agree</i> )
<i>IT expertise</i> * (Bhattacharjee and Sanford 2006)	How much knowledge do you possess about the following technologies from a user's perspective: [mobile apps, e-mail technology, web browsers, malware/spyware in the mobile context, security apps] (1 = <i>novice</i> ; 4 = <i>intermediate</i> ; 7 = <i>expert, formative</i> )
<i>Income</i> *	Which is your monthly net income level? (1 = <i>no regular income</i> ; 2 = <\$500; 3 = >\$500–\$1,500; 4 = >\$1,500–\$2,500; 5 = >\$2,500–\$5,000; 6 = >\$5,000–\$10,000; 7 = >\$10,000)
* Controls	

We included age, income, and IT expertise as controls in our research model (see Figure 3), as recommended in previous research (Dias et al. 2010; Liang and Xue 2010; Venkatesh and Morris 2000). Moreover, we controlled for the perceived effort associated with protective actions since this construct is often considered as also potentially influencing individuals' protection intentions (e.g., Liang and Xue 2010). However, we excluded perceived effort from our main hypotheses regarding the coping appraisal because — in line with Rogers (1975) — our study focuses on individuals' beliefs about the efficacy of coping responses (i.e., perceived effectiveness and perceived self-efficacy).

### 3.3.1.2 Step 2: Behavioral Experiment and Interviews

In the experiment, information about the functionalities of a free version and a premium version of an IT security app was presented to the participants. They were then asked to decide whether they would take \$5 in cash or a license for a premium version of the security app (worth \$7.95) as a reward for their participation. In the experiment, we controlled for endowment and order effects by using four control groups (Plott and Zeiler 2005; Schwarz

1999), as shown in Figure 5 (see also Acquisti and Grossklags 2004). Regarding the endowment effect, one control group was given the security app license first and the other control group was given the cash first. The participants then had the option of exchanging their reward. In contrast, the participants in the order effect control groups were asked directly whether they wanted to choose the premium app license (\$7.95) or the cash (\$5), but the order in which the options were presented varied across the two order effect control groups.



**Figure 5: Control Groups in the Experiment**

Moreover, as shown in Figure 4, we also conducted personal mini-interviews in the second step. The interviews aimed at acquiring a better understanding of the mobile IT security decisions the participants made in the experiment by analyzing the extent to which the participants had already undertaken problem-focused actions in order to cope with mobile IT security threats. Therefore, the participants were asked to list how they had protected their mobile devices from mobile IT security threats. The semi-structured interviews were guided by two questions: What are the reasons for the decision you made in the experiment? Under what conditions would you have decided differently?

### 3.3.2 Sampling

Data were collected in two rounds. The first data collection took place between February 15 and April 6, 2016 (58 females and 70 males) and the second between August 10 and August 12, 2016 (15 females and 37 males). We used flyers to acquire participants at our university. A voucher with a minimum value of \$5 was offered as an incentive for participating. The study was conducted in a laboratory at the university. Of the 73 female and 107 male mobile Android users who participated, three (two females and one male) had to be subsequently removed from the sample because the interview indicated that they had not read the information about the security app. In sum, our data set included 177 mobile users, of which 106 were male (mean age = 24.6; median = 23.5; SD = 5.4) and 71 were female (mean age = 25.8; median = 24.0; SD = 6.1). Nine of the 177 mobile users decided not participate in the

final step. Thus, 169 personal interviews (average duration 4 minutes) were conducted and recorded for analysis (protocol, audio files). The demographic characteristics of the sample used in this study are shown in Table 2.

**Table 2: Demographic Sample Characteristics**

<b>Age</b>	<i>n</i>	<i>Share</i>	<b>Education</b>	<i>n</i>	<i>Share</i>	<b>Gender</b>	<i>n</i>	<i>Share</i>
18–23	82	46.3%	Less than high school	2	1.1%	Female	71	40.1%
24–29	77	43.5%	High school degree	9	5.1%	Male	106	59.9%
30–35	12	6.8%	College degree	72	40.7%			
>35	6	3.4%	Undergraduate degree	62	35.0%			
Mean	25.1		Graduate degree	21	11.9%			
Median	24.0		Doctoral degree	1	0.6%			
SD	5.7		Other	10	5.9%			

### 3.3.3 Data Analysis and Results

#### 3.3.3.1 Assessment of Measurement Validations

First, we conducted the Shapiro-Wilk test separately for the data from the female sample and the data from the male sample. The results showed that in the female sample, perceived effectiveness and perceived susceptibility were not normally distributed and that in the male sample, perceived severity, perceived effectiveness, and perceived self-efficacy were not normally distributed. We compared the results of the first and the second round as well as the first and last 25% within the samples for the two rounds to test whether interest in the topic had any influence (Armstrong and Overton 1977). The non-parametric Mann-Whitney-U Test showed that no significant differences existed. We used the partial least square (PLS) method to evaluate our research model, following the guidelines proposed by Hair et al. (2013). The PLS method is appropriate for analyzing our research model due to the (partial) non-normality of our data and the explorative nature of our study (Hair et al. 2013). With  $n = 71$  for the female sample and  $n = 106$  for the male sample, our sample size meets the rule of thumb that suggests sample sizes larger than ten times the maximum number of paths directed to a particular construct in the measurement model (Barclay et al. 1995). The model was separately evaluated for male mobile users and female mobile users using SmartPLS software (SmartPLS 2016).

**Table 3: Indicator Reliability**

Indicators	Females		Males	
	Loadings	Indicator Reliability	Loadings	Indicator Reliability
Susc1	0.882	0.778	0.859	0.738
Susc2	0.787	0.619	0.856	0.733
Susc3	0.791	0.626	0.810	0.656
Sev1	0.901	0.812	0.851	0.724
Sev2	0.940	0.884	0.919	0.845
Sev3	0.814	0.663	0.575	0.331
Risk1	0.894	0.799	0.855	0.731
Risk2	0.728	0.530	0.814	0.663
Risk3	0.748	0.560	0.723	0.523
Effective1	0.947	0.897	0.900	0.810
Effective2	0.900	0.810	0.972	0.945
Self-eff1	0.940	0.884	0.939	0.882
Self-eff2	0.868	0.753	0.843	0.711
Self-eff3	0.857	0.734	0.891	0.794
Int1	0.933	0.870	0.932	0.869
Int2	0.938	0.880	0.932	0.869
Int3	0.892	0.796	0.879	0.773

Following the guidelines for PLS usage (Hair et al. 2013), parameters for indicator reliability (Table 3), composite reliability (CR, Table 4), and average variance extracted (AVE, Table 4) were computed in the next step in order to ensure convergent validity. With one exception in the male sample (Sev3: indicator reliability = 0.331), the indicator reliability values for all indicators exceed the minimum acceptable level of 0.4 and are close to or greater than the preferred level of 0.7 (Table 3) (Hulland 1999). With one exception (male sample, perceived severity: Cronbach's alpha = 0.687), the values for Cronbach's alpha (CA) all exceed the recommended threshold level of 0.7 (Nunnally et al. 1967) (see Table 4). However, the composite reliability values for perceived severity in the male sample and all other constructs are well above the recommended threshold of 0.7 (Bagozzi and Yi 1988), confirming the internal consistency of the constructs. For all measured constructs, the average variance



extracted values are above 0.5 in both the male sample and the female sample (Quan-Haase and Young 2010). Furthermore, we conducted the Fornell-Larcker criterion analysis for checking discriminant validity (Fornell and Larcker 1981) (Table 4). The results showed that in the female as well as the male sample the square root of the AVE for each construct is greater than the correlation of the construct with any other construct in the model. Overall, convergent and discriminant validity can be assumed.

**Table 4: Quality Criteria for the Constructs and Fornell-Larcker Criterion Analysis**

	AVE	CR	CA	SUS	SEV	R	EFF	SE	I
Susceptibility (SUS)	0.675 <i>0.709</i>	0.861 <i>0.880</i>	0.779 <i>0.797</i>	<b>0.821</b> <i>0.842</i>					
Severity (SEV)	0.787 <i>0.634</i>	0.917 <i>0.834</i>	0.862 <i>0.687</i>	0.386 <i>0.239</i>	<b>0.887</b> <i>0.796</i>				
Risk (R)	0.629 <i>0.639</i>	0.835 <i>0.841</i>	0.710 <i>0.714</i>	0.320 <i>0.433</i>	0.542 <i>0.652</i>	<b>0.793</b> <i>0.799</i>			
Effectiveness (EFF)	0.853 <i>0.877</i>	0.921 <i>0.934</i>	0.831 <i>0.871</i>	-0.053 <i>0.179</i>	0.095 <i>0.062</i>	0.096 <i>0.202</i>	<b>0.924</b> <i>0.937</i>		
Self-efficacy (SE)	0.790 <i>0.796</i>	0.919 <i>0.921</i>	0.868 <i>0.874</i>	-0.466 <i>-0.281</i>	-0.187 <i>-0.031</i>	-0.089 <i>-0.099</i>	0.099 <i>-0.125</i>	<b>0.889</b> <i>0.892</i>	
Intention (I)	0.849 <i>0.837</i>	0.944 <i>0.939</i>	0.911 <i>0.902</i>	0.006 <i>-0.094</i>	0.280 <i>0.209</i>	0.333 <i>0.225</i>	0.410 <i>0.010</i>	0.152 <i>0.447</i>	<b>0.921</b> <i>0.915</i>
Note: The results for the female subsample are displayed in standard font and the results for the male subsample are displayed in grey italic.									

**Table 5: Collinearity Statistics**

Constructs	Females		Males	
	Tolerance	VIF	Tolerance	VIF
Susceptibility	0.851	1.175	0.943	1.060
Severity	0.851	1.175	0.943	1.060
Risk	0.946	1.057	0.938	1.066
Effectiveness	0.963	1.038	0.905	1.105
Self-efficacy	0.971	1.030	0.766	1.305
Intention	0.873	1.145	0.757	1.321

To test for multicollinearity, we calculated the tolerances and variance inflation factor (VIF) values separately for the female and male samples. The results are shown in Table 5. The tolerance values all exceed the recommended threshold of 0.2 and the VIFs are all below the recommended threshold of 5 (Hair et al. 2011). Thus, we can rule out collinearity problems for our model.

### 3.3.3.2 Behavioral and Qualitative Data

Only 53 of the 177 participants (29.9%) in the experiment chose the premium security app license as a reward for participating in our study; 28 of these were female and 25 were male. 124 participants (70.1%) decided to take the cash (43 females and 81 males). The Kruskal-Wallis Test showed that the endowment and order effect did not have any influence on the participants' choices in the experiment, i.e., on their decisions whether to choose the premium security app license or the cash (chi-square = 1.838, df = 3, asymp. Sig. = 0.607). The Mann-Whitney-U Test showed that the decisions made in the experiment were significantly different for the male and female mobile users (asymp. sig (2-tailed) = 0.035). Specifically, female users were found to be more likely to choose the security app license. However, the participant's choices in the experiment may have been influenced by their previous coping actions. For example, if a participant had already taken safeguarding measures that provide the same level of protection as the offered security app, the participant's decision to take the cash cannot be interpreted as non-secure behavior. Therefore, we combined the data gathered in the personal interviews and the data from our quantitative study in order to evaluate the actual security behavior of the participants.

Eight females and one male did not participate in the interviews. Accordingly, data about the participants' actual IT security behavior is measured only for 168 data sets (63 females and 105 males). The actual IT security behavior of the participants was classified into three levels of problem-focused coping behavior: low, medium, and high. As result of discussions between three IS researchers, the assignment of the participants to one of the three coping behavior levels was done in three steps. In the first step, the behavioral data from the experiment were used. If a participant chose the premium security app license, he or she was considered as showing a high level of problem-focused coping. If the participant chose the cash, we included information about the participant's previous coping actions (i.e., safeguarding measures already taken) in the actual behavior evaluation. We checked whether this participant stated in the prior survey that he or she had installed a free security app, a premium version of a security app, or no security app. If the participant had already installed a

premium version of a security app, his or her decision was also interpreted as showing a high level of coping behavior. For the other two cases (i.e., “free version of a security app installed” and “no security app installed”), we additionally included the qualitative data from the personal interviews to evaluate the participants’ actual coping behavior in a third step. In the qualitative interviews, two groups of other technical security measures were mentioned by the participants: system-internal security solutions and open-source security solutions. If a participant argued in the interviews that he or she utilizes such a technical security measure (“I use the CyanogenMod Operating System and I don’t have Google Play Store installed,” “I prefer using a tool like XPrivacy or the embedded functions in CyanogenMod”), the participant was also assigned to the group that shows a high level of problem-focused coping. Installation of a free version of a security app was considered to be medium problem-focused coping behavior, and taking no safeguarding measure a low level of problem-focused behavior (“I didn’t need a security app until now”, “Only pictures are important to me. These get automatically synchronized with Google Drive. Therefore, the pictures are secured”, “I am concerned that the app will slow down the performance of my smartphone and interfere with my web browsing experience”). The level classification is shown in Table 6 for both male and female mobile users.

**Table 6: Classification of Actual Problem-Focused Coping Behavior**

<b>Problem-focused coping behavior</b>	<b>Females (n=63)</b>	<b>Males (n=105)</b>	<b>Total (n=168)</b>
<b>Low</b>	25 (35.2%)	41 (38.7%)	66 (37.3%)
<b>Medium</b>	10 (14.1%)	26 (24.5%)	36 (20.3%)
<b>High</b>	28 (39.4%)	38 (35.8%)	66 (37.3%)

### 3.3.3.3 Structural Model Testing

In the next step, we evaluated our structural model (Figure 3) separately for the female sample and the male sample. Our model explains 30.8% of the variance in perceived threat in the female sample and 50.7% in the male sample. The variance explained in mobile users’ protection intention is 51.6% for females and 41.3% for males. Regarding the observed protective actions, 24.9% of the variance is explained in the female sample and only 8.3% in the male sample. Given the explorative nature of our study, the values for  $R^2$  and their corresponding discrepancies between the female and the male sample show that the level of explanatory power for our research is appropriate.

**Table 7: Results of Structural Model Testing**

Hypothesis	Results	Path Coefficients	
		Females	Males
<i>H1a: Perceived severity → perceived threat</i>	Supported: same for males and females	<b>0.492***</b>	<b>0.582***</b>
<i>H1b: Perceived susceptibility → perceived threat</i>	Supported: stronger for males	0.130	<b>0.294**</b>
<i>H1c: Perceived threat → protection intention</i>	Not supported: same for males and females	<b>0.348***</b>	<b>0.223**</b>
<i>H2a: Perceived effectiveness → protection intention</i>	Not supported: stronger for females	<b>0.277***</b>	0.064
<i>H2b: Perceived self-efficacy → protection intention</i>	Supported: stronger for males	0.027	<b>0.222***</b>
<i>H3: Protection intention → coping actions</i>	Not supported: stronger for females	<b>0.417*</b>	0.226
Note: *p < 0.05; **p < 0.01; ***p < 0.001.			

The path coefficients in our structural model and their significance levels were calculated based on the PLS method and a bootstrapping procedure (5000 subsamples, no sign changes, pairwise deletion). The results are summarized in Table 7. We found that perceived severity has a significant positive association with perceived threat for both male and female mobile users (female:  $\beta = 0.492$ , p-value = 0.000; male:  $\beta = 0.582$ , p-value = 0.000). To assess whether the path coefficients for this significant relationship are different for male and female mobile users, we utilized a multi-group analysis (MGA) procedure. This did not reveal any significant differences in the association of risk severity with males and with females, supporting H1a (p-value = 0.777). In contrast, with respect to perceived susceptibility, the results show a significant positive association with perceived threat for male mobile users but not for females (female:  $\beta = 0.130$ , p-value = 0.313; male:  $\beta = 0.294$ , p-value = 0.001). Accordingly, as the positive effect of perceived susceptibility on perceived threat is stronger for males, H1b is also supported. Regarding H1c, the results show that perceived threat is significantly positively associated with protection intentions for both female and male mobile users (female:  $\beta = 0.348$ , p-value = 0.000; male:  $\beta = 0.223$ , p-value = 0.008). Contrary to our expectation, the MGA procedure showed no significant differences in the path coefficients (p-value = 0.147) for females and males. Thus, H1c is not supported. While perceived effectiveness was found to have a significant positive association with protection intentions for female but not for male mobile users (female:  $\beta = 0.277$ , p-value = 0.000; male:  $\beta = 0.064$ , p-value = 0.458), the positive association of perceived self-efficacy with the protection

intention is only significant for male mobile users (female:  $\beta = 0.027$ ,  $p\text{-value} = 0.777$ ; male:  $\beta = 0.222$ ,  $p\text{-value} = 0.008$ ). Thus, H2a is not supported and H2b is supported. The positive relationship between mobile users' stated protection intention and observed actual coping actions is significant for females but not for males (female:  $\beta = 0.417$ ,  $p\text{-value} = 0.002$ ; male:  $\beta = 0.226$ ,  $p\text{-value} = 0.052$ ). Even though the influence of protection intentions on coping actions is very close to the 5% significance level, H3 cannot be supported.

Finally, we did not find a significant influence of the control variable age on protection intentions (female:  $\beta = 0.061$ ,  $p\text{-value} = 0.369$ ; male:  $\beta = 0.029$ ,  $p\text{-value} = 0.683$ ) or on participants' coping actions (female:  $\beta = -0.141$ ,  $p\text{-value} = 0.217$ ; male:  $\beta = 0.066$ ,  $p\text{-value} = 0.597$ ). The influence of income on protective actions is positively significant for females but not for males (female:  $\beta = 0.274$ ,  $p\text{-value} = 0.010$ ; male:  $\beta = -0.215$ ,  $p\text{-value} = 0.058$ ); moreover, the relationship is negative in the male sample. IT expertise is found to significantly positively influence males' but not females' protection intentions (female:  $\beta = -0.213$ ,  $p\text{-value} = 0.234$ ; male:  $\beta = 0.285$ ,  $p\text{-value} = 0.006$ ). Regarding the influence of IT expertise on the actual coping actions, no significant relationship in either the female or the male sample is found (female:  $\beta = 0.004$ ,  $p\text{-value} = 0.980$ ; male:  $\beta = -0.070$ ,  $p\text{-value} = 0.621$ ). The negative relationship between perceived effort and protection intention is significant for both female and male mobile users (female:  $\beta = -0.393$ ,  $p\text{-value} = 0.000$ ; male:  $\beta = -0.265$ ,  $p\text{-value} = 0.002$ ). The path coefficients for the male and female subsamples do not differ significantly ( $p\text{-value} = 0.838$ ).

### 3.4 Discussion

In this study, we analyzed the differences between male and female mobile users in cognitive IT security appraisals and protective actions. Based on the theoretical underpinnings of PMT and Gender Schema Theory, we first derived a variance model of mobile users' coping behavior. Then we conducted a survey and an experiment with mobile users, followed by personal interviews. The results of our study show that gender differences play an important role in the cognitive processes that predict mobile users' protection intentions and protective behaviors. We found that the protection intentions of male and female mobile users are based on different underlying cognitive processes in the threat appraisal and the coping appraisal. Moreover, the results indicate that male mobile users fail to take the necessary protective actions even though they actually intend to protect their devices from mobile IT security threats.

Specifically, with respect to the threat appraisal, females' perceptions of threats were found to be primarily predicted by their perceptions of the severity of an incident, while males additionally based their threat perceptions on their perceived susceptibility (i.e., the likelihood that an incident would happen to them). Accordingly, it can be assumed that females tend to perceive a mobile security threat as high as soon as they perceive it to be associated with a certain degree of damage, even if the negative event is actually very unlikely to occur. One reason for this finding could be that female mobile users are less certain when it comes to the assessment of IT security threats. While perceived susceptibility is strongly based on technical configurations, the severity of a negative event does not necessarily require specific knowledge about IT security. In line with Gender Schema Theory (Bem 1981), it can be concluded that the information about risk susceptibility and risk severity that is available to mobile users is processed differently by females and males because they have different associations with such information. For example, females might be more emotionally upset than males when thinking about an attack on the sensitive data stored on their mobile devices. Accordingly, females would be likely to evaluate this mobile IT security threat as high without considering the probability that the event might occur. In contrast, males will in addition process information about their perceived susceptibility when appraising the threat. Moreover, the explained variance of the perceived threat is much lower in the female sample (30.8%) than in the male sample (50.7%). This may indicate that further factors exist that need to be considered as antecedents of female mobile users' perceived threat. Contrary to our expectation, we did not find significant differences between females and males in the relationship between mobile users' perceived threat and protection intentions. In both the female and the male sample, the perceived mobile threats were found to significantly positively influence mobile users' protection intentions. One reason for this finding could be that both females and males are well aware of the danger of IT security threats because the importance of IT security is widely accepted in society and the topic is continually receiving increased attention from the media. Accordingly, raising the perceived levels of mobile security threats will result in a strengthening of both female and male mobile users' intentions to take protective action. However, while females' levels of threat perception can be raised by emphasizing the severity of the damage that can result from mobile IT security incidents, raising males' perceived levels of threat requires emphasizing both the associated damage and their perceived probability that the mobile IT security incidents will happen to them.

Even though gender differences were found in mobile users' coping appraisal with respect to the perceived effectiveness of safeguarding measures, the positive relationship between

perceived effectiveness and protection intentions was found to be significant for females but not for males. This is contrary to our expectation that because males are more task-oriented and more motivated by achievement, they would therefore be more likely to base their protection intention on the perceived effectiveness of a safeguard. However, the positive relationship between perceived self-efficacy for coping with a threat and protection intentions is only significant for males. In sum, our results indicate that females' coping appraisal is based primarily on the perceived effectiveness associated with protective behavior, while males' coping appraisal is primarily based on their perceived self-efficacy to cope with the threat. Accordingly, when deciding about coping with a risky situation, a female mobile user will base her decision on the perceived capabilities of a safeguard to effectively reduce the perceived risk, while a male mobile user will base his decision on his own capabilities (i.e., his perceived self-efficacy). One reason for this result could be that males are more "self-congratulatory" than females (Pajares 2002) and thus may tend to base their coping appraisals more strongly than females do on their assessments of their own capabilities.

Overall, the results show that the cognitive processes that are assumed by PMT explain a substantial portion of the variance in mobile users' protection intentions. Nevertheless, the variance in mobile users' protection intentions explained by our research model is higher for females than for males. Therefore, one can ask whether males base their protection intentions more strongly on other factors, such as affective factors.

With respect to mobile users' actual behavior, the results of the experiment indicate that females are more likely than males to show problem-focused coping behavior, i.e., to adopt an IT security safeguard for their mobile devices when they intend to protect their mobile devices. In particular, we did not find a significant relationship between protection intentions and the implementation of technical IT security measures in the male sample but we did find one in the female sample. As such, our results show that male users tend to be less likely to confront mobile IT security threats head-on and to show problem-focused coping actions. Thus, the question arises whether males are more likely to apply emotion-focused coping strategies in response to mobile IT security threats. In this case, males would be more emotionally driven in the context of mobile IT security. The variance in mobile users' protective behavior that is explained by their protection intentions is three times less for the male sample than for the female sample. This indicates that the problem-focused behavior of males is influenced by other, additional factors. For example, males could include their perceived control over the data stored on their mobile devices in their decision-making about

coping behavior and therefore be more likely to be vulnerable to perception bias, e.g., the systematic underestimation of risks. When males — the more self-confident and self-congratulatory gender — overestimate their control over the data stored on their mobile devices, they refrain from implementing necessary IT security measures and show less problem-focused coping behavior. As such, our results indicate that males are more likely to engage in risky behavior regarding how they use their mobile devices and less likely to show problem-focused coping actions. This contradicts the widespread assumption in a large stream of research that females — the more emotional gender — are more likely to apply emotion-focused coping strategies while males are more likely to apply problem-focused coping strategies (Pearlin and Schooler 1978; Stone and Neale 1984). However, Tamres et al. (2002) found in their meta-review of literature dealing with gender differences in coping behaviors that the findings of studies on gender-specific coping behavior are often inconsistent, so that the widespread assumption of problem-focused males and emotion-focused females in the context of coping behavior needs to be rethought. For example, in certain situations (e.g., in coping with relationship stressors) males have been found to apply more emotion-focused coping strategies (Tamres et al. 2002), and in the context of personal health behavior, females have been found to be more likely to engage in problem-focused coping behavior (Tamres et al. 2002). According to Tamres et al. (2002), one reason for these findings regarding problem-focused and emotion-focused coping behaviors in females and males might be that males often exhibit two opposite stereotypes: On the one hand, males are assumed to be more likely to confront a problem head-on, while on the other hand, males have also been found to be the gender that is more likely to deny that a problem exists (Tamres et al. 2002). Based on the results of their meta-analytic review, Tamres et al. (2002) conclude that these opposite stereotypes of males might be explained by the situational context. As such, they presume that males may particularly exhibit less problem-focused coping behaviors in situations in which a threat is perceived as less controllable (e.g., in interpersonal relationships). Considering that our study found that perceived effectiveness of technical IT security measures does not have a significant influence on males' protection intentions, it could be speculated that males perceive mobile IT security threats as less controllable than do females. As a result, males would be more likely to conclude that a threat cannot be avoided. To maintain psychological balance, the perceived threat level is lowered by denying that the problem exists ("It won't happen to me") or by other wishful thinking ("Nobody would be interested in stealing my information") (Liang and Xue 2009).



Moreover, our results indicate the presence of an intention–behavior gap for male mobile users. Previous studies have similarly shown that individuals may behave inconsistently with self-reported intentions regarding their privacy and security (e.g., Acquisti and Grossklags 2004; Belanger et al. 2002; Norberg et al. 2007). In this context, the question arises whether this paradoxical intention–behavior relationship is similar to the so-called Privacy Paradox (Dinev and Hart 2006; Norberg et al. 2007). However, the intention–behavior relation seems to be slightly different in context of our study: While this study analyzes people’s behavior with regard to protecting their privacy (i.e., by implementing safeguarding measures), the Privacy Paradox focuses on people’s decisions to surrender a certain degree of privacy in exchange for outcomes (Dinev and Hart 2006). Nevertheless, the reasons for the paradoxical behavior of male mobile users need to be understood in order to ensure that it is not only females who actively protect their mobile devices, their private data repositories.

This study has several important theoretical implications. Overall, this paper extends existing research on the IT security behavior of individuals by being the first to examine how mobile users’ gender influences their threat and coping appraisals as well as their consequent coping behaviors. This paper shows that the underlying cognitive assessments (i.e., the effects of the threat and coping appraisals) on which protection intentions are based differ between female and male mobile users. This finding highlights the importance of considering users’ gender when analyzing coping behaviors in the context of IT security. Ignoring the important role of users’ gender may lead to misleading results. For example, since females are still an underrepresented population in the IT workforce (Bagchi-Sen et al. 2010), the results of IT security research in the organizational context are often based on data primarily gathered from males. Considering the results of our study, findings that are based on existing IT security research may be correct for males but not for females. Moreover, in contrast to most other studies in IS research, this study not only analyzes the way mobile users build their protection intentions but also observes the corresponding actual coping behaviors. In this context, the results of the experiment and interviews indicate that male mobile users are less likely to translate their stated protection intentions into problem-focused coping behavior. This type of intention–behavior gap is well-recognized in behavioral research (e.g., Norberg et al. 2007; Sheeran 2002) and highlights the importance of conducting more experiments in IT security perception and behavior research. In particular, we still do not have a good understanding of *why* individuals fail to effectively protect themselves even in cases with minimal cost. Factors mediating and moderating the relationship between protection intentions and protective actions need to be identified and analyzed to gain a better understanding of individuals’ actual

protection behavior and thereby ultimately increase the security levels of mobile users. Furthermore, while it can be noted that PMT is a valid theoretical lens for analyzing protection intentions and behavior in the context of mobile IT security, we also found that the relationships between the constructs assumed by PMT and mobile users' protection intentions are different for females and males. As such, this study not only extends our theoretical understanding of the cognitive processes that predict females' and males' intentions to behave securely but also shows that the validation of theories in IT security that are based on individuals' cognitive processes can be strongly influenced by individuals' gender. This finding might provide an explanation for the contradictory findings in previous research that uses PMT in the IT security context. For example, while Herath and Rao (2009b) and Johnston and Warkentin (2010) found that only severity had a significant influence on the perceived threat, Lee et al. (2008) found that only susceptibility was significant, and Liang and Xue (2010) found significant influences of both severity and susceptibility on individuals' perceived threat. Although some of these studies include gender as a control (e.g., Herath and Rao 2009b; Liang and Xue 2010), they do not consider the influence of gender on the paths between the cognitive constructs assumed in PMT.

This study also has several implications for mobile users and practitioners, such as suppliers of IT security and organizations in general. Female mobile users can learn from this study that they should consider their perceived susceptibility to a greater degree in their threat appraisals in order to avoid overestimation of a threat and subsequent ineffective decisions. Male mobile users can learn that they do not sufficiently consider the perceived effectiveness of available security measures in their coping appraisals. Moreover, our results indicate that mobile users — especially male mobile users — do not necessarily behave as securely as they originally intended. Accordingly, this study may sensitize mobile users to the fact that they should carefully consider whether the safeguarding measures they have taken for their mobile devices are adequate to ensure the security level they intend to achieve for their smartphones. For suppliers of IT security products, it is essential, when designing marketing campaigns, to consider that males and females cope differently with IT security threats. In particular, marketing messages for male mobile users should also underline the likelihood of an incident and encourage users' self-efficacy. Moreover, the results of the experiment and the interviews indicate that IT security suppliers should focus not only on customers' perceptions of the product characteristics influencing their protection intentions but also the factors that influence customer's translation of their intentions into protective behavior (e.g., buying a security app). Organizations can use the results of this study regarding the different

underlying processes influencing the protection intentions of female and male mobile users when developing educational programs. The fact that users are often considered to be the weakest link in organizations' IT security (e.g., Bulgurcu et al. 2010) particularly highlights the need for gender-specific training and educational programs addressing the specific impact factors that are relevant in females' and males' IT security perceptions and coping behaviors. For example, awareness programs aiming to raise the intention of employees to secure the organizational IT systems should especially emphasize the severity of the potential damage in the case of an IT security incident within the organization and the effectiveness of the coping behavior that is specified in the organization's IT security policies. Neglecting gender differences in females' and males' cognitive appraisals when educating them about how to cope with IT security threats confronting the organization might result in investments that will not pay off as much as they could.

### **3.5 Limitations and Future Research**

Three limitations of this study merit consideration. First, the results of the empirical analysis are based on data from users of only one mobile operating system (Android) and a student sample. However, even though the Android operating system still dominates the market, further research could nevertheless enrich the results of this study by verifying these results in additional quantitative and experimental studies with more representative samples and different operating systems. These studies could also further analyze gender-specific reasons for the different cognitive and affective processes by considering additional gender-specific personality traits (e.g., self-regulation and overconfidence). Second, this study does not analyze security perceptions and behaviors longitudinally. The threat and coping appraisals may change over time due to new information. For example, a user's peer (e.g., a family member, friend, or colleague) might become a victim of a security incident, or the user might learn new information about security threats through the media. As a consequence, the perceptions of security threats and safeguarding measures might be influenced, which in turn would influence protection intentions and respective coping behaviors. Accordingly, we encourage future research to conduct longitudinal studies and thereby analyze the perceptions and behaviors of female and male mobile users at various points in time. This may also enable researchers to better understand the different underlying cognitive processes within males' and females' threat and coping appraisals and potential changes over time. Third, the results of this study regarding the relationship between the measured protection intention in the first research step (survey) and the coping behavior observed in the second research step

(experiment and interviews) have to be interpreted carefully. Specifically, while the measured protection intention of the participants was formulated as the goal of protecting a smartphone and the data stored on it, the observed coping behavior was limited to single actions regarding the implementation of technical security measures. Despite our use of a behavioral experiment and personal interviews to correctly capture the problem-focused coping actions of the participants as much as possible, we cannot say with certainty that we succeeded. Moreover, we did not measure emotion-focused responses. Accordingly, additional experiments are required to further analyze the gender-specific relationship between mobile users' stated protection intentions and their actual coping behaviors as well as gender-specific applications of emotion-focused and problem-focused coping strategies.

## 4 Research Paper B: Top Managers' IT Security Awareness

**Title:** The Role of Top Managers' IT Security Awareness in Organizational IT Security Management

**Authors:** Sonnenschein, Rabea  
Loske, André  
Buxmann, Peter

**Published in:** Proceedings of the 38<sup>th</sup> International Conference on Information Systems (ICIS), Seoul, South Korea 2017

### Abstract

*Despite the widely recognized importance of top managers' IT security awareness for effective IT security management, previous research has paid little attention to its complex nature. Against this backdrop, we conducted a structured literature review to identify and organize factors that have been found to determine managerial IT security awareness. Particularly, a systematic consolidation of the literature streams in combination with expert interviews and Q-sorting revealed that individual- and organization-related factors form two distinct dimensions of managers' IT security awareness. Within the qualitative evaluation, we identified two supplementary factors (one in each dimension). Further, we found that the awareness of both top managers and managers at the department level is crucial for effective IT security management. Our proposed conceptualization will enable both researchers and practitioners to better understand managers' IT security awareness and to subsequently develop interventions dedicated at improving managers' awareness and thus the effectiveness of IT security management.*

**Keywords:** IT Security, Management, Awareness, Effectiveness, Literature Review.

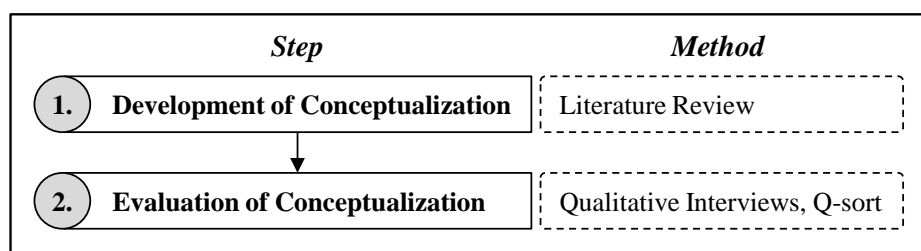
## 4.1 Introduction

Nowadays, the protection of sensitive data and information technology (IT) systems from security incidents represents one of the major challenges for organizations. The costs for data leakage, lost productivity, and long-term reputational damage can be huge and therefore, a single security breach can even threaten an organization's existence. Fittingly, Ginni Rometty, chairman, president and CEO of IBM stated at the IBM Security Summit in 2015 that cybercrime "is the greatest threat to every profession, every industry, every company in the world" (Forbes 2015a). This statement also reflects findings of recent statistics. According to Statista, the average financial loss of large organizations due to IT security incidents was \$3.9 million in 2013 and increased to \$5.9 million in 2014. The worldwide damage for cybercrime is predicted to hit \$6 trillion annually by 2021, up from \$3 trillion in 2015 (Cybersecurity Ventures 2016). The number of security incidents is constantly rising and an opposing trend is not foreseeable. Compared to 2014, the number of detected security incidents increased by roughly about 38 percent in 2015 (Socialnomics 2016). For IT security experts, these statistics are frustrating — not only because they demonstrate the increasing sophistication of attackers, but also because effective safeguards would have been readily available in many cases but were obviously not implemented in the organizational IT systems. According to the 'Data Protection & Breach Readiness Guide' of the Online Trust Alliance (OTA), 91 percent of the data breaches in 2015 could have been prevented (OTA 2016). By way of example, experts claim that the Sony Pictures hack in 2014 could have been easily prevented by mail encryption (Virtru 2015). Another example is given by the IRS hack where hackers gained access to personal data from more than 700,000 taxpayer accounts (The Wall Street Journal 2016). Experts assume that this incident could have been easily prevented with the implementation of two-factor authentication (Forbes 2015b). Thus, those specialists responsible for the organization's IT security actually should have been aware about the existence of the necessary safeguarding measures. However, previous studies have found that IT security specialists' scope for action (e.g., the IT security budget) within an organization is often too restricted due to a lack of top management support, so that they cannot effectively secure the organizations' IT systems (pwc 2015). As such, top managers' IT security awareness plays a central role in effective IT security management as well (e.g., Ashenden 2008; Choi et al. 2008; Sharma and Yetton 2007). If the top management is not aware about the threats their organization faces with respect to IT security, the topic will not be of high priority when it comes to decisions about resource allocations. Against this backdrop, previous studies have demonstrated that top managers are not well prepared for the higher

complexity of IT security risks arising from trends, such as Big Data and Cloud Computing (EMC 2014). In order to overcome the problem of organizations' insufficient protection levels against IT security risks, it is essential to improve the awareness about IT security at the top management level. Thus, to ensure effective IT security management, it is necessary to understand the nature and role of top managers' IT security awareness.

Previous IS research repeatedly highlighted the important role of the top management in an effective IT security management (e.g., Hu et al. 2012; Kankanhalli et al. 2003; Sharma and Yetton 2007). It is argued that top management attention and commitment to IT security positively influences the IT security level of an organization because the greater top management support in an organization the more resources will be allocated for IT security management (Herath and Rao 2009b; Kankanhalli et al. 2003). Moreover, it is commonly assumed that managerial actions toward IT security (e.g., information security policies or security trainings) increase employees' IT security awareness (Albrechtsen and Hovden 2010; Haeussinger and Kranz 2013; Spears and Barki 2010) and therefore, enhances employees' IT security behavior (e.g., Bulgurcu et al. 2010; Hu et al. 2012). As such, a top-down effect from the management level to the employee level is proposed (e.g., Kritzinger and Smith 2008). Although the importance of top managers for effective IT security risk management in organizations is widely recognized (e.g., Ashenden 2008; Sharma and Yetton 2007), research on the nature and role of top managers' IT security awareness is still rare. The extant literature is predominantly focused on employees' IT security awareness and largely neglects the awareness of top managers in organizations (e.g., Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009a; Posthumus and Von Solms 2004; Vance et al. 2012). Moreover, those few studies dealing with IT security awareness at the top management level tend to focus on either individual-related factors (e.g., top managers' individual knowledge about IT security risks and controls) or organization-related factors (e.g., top managers' perception of industry-specific sensitivity of data and IT systems). An exhaustive conceptualization that includes individual- as well as organization-related factors of the concept of top managers' IT security awareness in IT security management is still missing. To address this research gap, we follow the call for research by Haeussinger and Kranz (2017) and focus our study on the concept of IT security awareness at the top management level. It can be assumed that factors determining this concept at the top management level differ from factors at the employee level, for example due to different responsibilities of employees and top managers (see also Siponen 2001). We chose a two-step research approach (see Figure 6). First, we develop a conceptualization of top managers' IT security awareness based on a structured literature

review and insights from related research streams. The proposed conceptualization considers both factors representing the individual dimension and factors representing the organizational dimension of top managers' IT security awareness as well as its role in an organization's IT security management. In our second step, we evaluate the developed conceptualization using qualitative expert interviews with multiple IT security experts from different hierarchical levels in an organization as well as with IT security suppliers. In addition, the validity of the proposed conceptualization is confirmed by applying the Q-sort method.



**Figure 6: Research Approach (Research Paper B)**

By developing and evaluating an exhaustive conceptualization of top managers' IT security awareness, this work makes significant contributions to IS research and practice. First of all, the study contributes to the emerging body of IT security awareness literature by highlighting and confirming the important role of IT security awareness at the top management level for an effective IT security management in organizations. Based on the structured literature review, we identify and organize factors that have been found to determine top managers' IT security awareness in the extant literature. These factors are empirically evaluated and validated with expert interviews and Q-sorting. This second step revealed two additional factors that are relevant to top managers' IT security awareness but have been disregarded by previous studies: previous IT security experience and legal requirements. Additionally, since we found that not only the IT security awareness of top managers is crucial for effective IT security management but also the awareness of managers at the department level, our results indicate that future research should consider all hierarchical levels of an organization when studying IT security management. The resulting conceptualization provides a basis for future research to better understand the formation of organizational IT security investment decisions. From a practitioner's perspective, our study clearly shows that not only top managers but all managers throughout the entire organization must be aware of IT security and their important roles in establishing effective IT security management. Specifically, our findings emphasize that the combination of decision-making power (i.e., scope for action) and IT security knowledge is crucial for effective IT security management. Therefore, organizations should identify and integrate appropriate positions in their organizational structure to increase their



overall IT security level (Wu and Saunders 2005). Further theoretical and practical implication will also be discussed.

## **4.2 Step 1: Development of Conceptualization**

### *4.2.1 Overview of Related Literature Streams*

Since employees are often considered to be the weakest link in an organization's IT security, many researchers have focused their studies on the employee level. Specifically, the antecedents of employees' information security policy compliance and noncompliance behaviors are extensively analyzed (see e.g., Abdul Talib and Dhillon 2015; Bulgurcu et al. 2010; Siponen et al. 2010; Siponen and Vance 2010; Vance et al. 2012). Within their systematic review of quantitative studies in employees' information security policy compliance, Sommestad et al. (2014) identify more than 60 variables that have been investigated by previous research. 40 of these 60 variables were only analyzed in a single study whereas the most popular variables in previous research are subjective norm, self-efficacy, and perceived severity of sanctions (Sommestad et al. 2014).

Several studies analyze the effect of employees' IT security awareness on their compliance behavior (e.g., Bulgurcu et al. 2010; D'Arcy et al. 2009; Vance et al. 2012). Employees' IT security awareness is commonly defined in previous research as the extent to which employees are aware of and committed to their organizations' IT security objectives (e.g., Siponen 2000a). For example, Bulgurcu et al. (2010) analyzed the impact of employees' IT security awareness (both IT security policy awareness and general IT security awareness) on their attitudes regarding compliance with their organizations' IT security policies. As such, within those studies the IT security awareness of employees is believed to be the key for effectively protecting an organizations data and IT systems (Goodhue and Straub 1991; Hu et al. 2007; Siponen 2000a; Siponen 2000b; Whitman 2004). Therefore, many researchers investigated the effect of different security education training and awareness (SETA) programs, such as IT security workshops and trainings (e.g., Puhakainen and Siponen 2010; Thomson and von Solms 1998) or learning tutorials (e.g., Chen et al. 2006). It is argued that SETA programs increase employees' IT security awareness (Albrechtsen and Hovden 2010; Haeussinger and Kranz 2013; Spears and Barki 2010) and are thus effective countermeasures for reducing employees' misbehaviors (Albrechtsen and Hovden 2010; D'Arcy et al. 2009; Peltier 2005; Spears and Barki 2010). In this context, Albrechtsen and Hovden (2010) show in their experimental research that employee participation enhances their IT security awareness

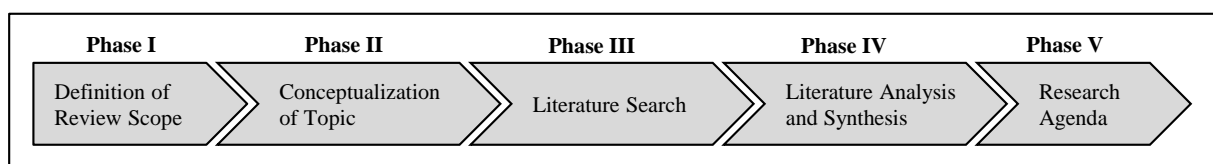
and consequently, their information security policy compliance behavior. The positive effect of employee participation through greater IT security awareness on the IT security of an organization is empirically tested and confirmed by Spears and Barki (2010).

Another research stream in this context deals with the so-called “IT security culture” of organizations (e.g., Dojkovski et al. 2010; Knapp et al. 2006; Ruighaver et al. 2007; Van Niekerk and Von Solms 2010). These studies have investigated information security from an organizational point of view and often highlight the importance of management attention and management support as success factors for effective IT security risk management in organizations (e.g., Ashenden 2008; Sharma and Yetton 2007). Ma and Ratnasingam (2008) analyze the influence of organizational characteristics such as firm size, financial commitment, and management support on IT security management. Uffen et al. (2012) focus on the influence of personality traits and other cognitive factors on IT security management. Kankanhalli et al. (2003) found in their empirical study among managers that organizations with stronger top management support engage in more preventive efforts to ensure IT security compared to organizations with weaker top management support.

Overall, findings from related research at the employee level indisputably demonstrate that IT security awareness is fundamental for effectively protecting the data and IT systems of an organization. However, even though previous research repeatedly highlighted the important role of the top management in an effective IT security management (e.g., Hu et al. 2012; Kankanhalli et al. 2003), studies investigating top managers' IT security awareness are still rare.

#### 4.2.2 Literature Review on Top Managers' IT Security Awareness

In accordance with the framework for conducting IS literature reviews suggested by Vom Brocke et al. (2009), we structured our literature review in five phases (see Figure 7): definition of review scope, conceptualization of topic, literature search, literature analysis and synthesis, and research agenda.



**Figure 7: Framework for Literature Reviewing (based on Vom Brocke et al. 2009)**

First, we defined our review's scope: we focus on IT security awareness at the top management level in the context of organizational IT security management (Phase I). Second,

we performed an explorative search using Google Scholar and the Business Source Premier to gain a conceptual understanding of the topic, to identify relevant journals, and to identify a relevant search term (Phase II). Third, we conducted a literature search using the selected search term (see Table 8; Phase III). As proposed by Vom Brocke et al. (2009), the literature search in Phase III involves database, keyword, backward, and forward search. We selected three databases that provide access to leading IS journals: the AIS Electronic Library (AISeL), ScienceDirect, and Business Source Premier. As our initial explorative search already showed that research within the managerial IT security awareness domain is rare, we decided to include journals, conference papers, and books in the review process (Webster and Watson 2002). The keyword search identified 1512 papers in total. Following the literature search process proposed by Vom Brocke et al. (2009), we then performed a title screening followed by an examination of the abstracts of the remaining papers. The title screening resulted in 445 papers and the abstract screening in 56 papers. Next, through a detailed reading of the 56 papers, we identified that only 15 of these papers deal with top managers' IT security awareness itself and its role in IT security management. Finally, we conducted a forward and backward search in accordance with Webster and Watson (2002), which resulted in the identification of one additional relevant paper. The results of the literature search (Phase III) are summarized in Table 8.

**Table 8: Overview of the Literature Search Process**

<b>Step</b>	<b><i>Keyword Search</i></b>	<b><i>Title Screening</i></b>	<b><i>Abstract Screening</i></b>	<b><i>Full Text Screening</i></b>	<b><i>Forward &amp; Backward Search</i></b>
<b>Papers Remaining</b>	1512	445	56	15	16
<b><i>Search Term</i></b>	(title: (managerial OR management OR organization) AND title: (security awareness OR ISA)) OR (abstract: (managerial OR management OR organization) AND abstract: (security awareness OR ISA))				

The results of Phase IV and Phase V of the framework for conducting IS literature reviews (Vom Brocke et al. 2009; see Figure 7) are presented in the remaining part of this paper.

#### 4.2.3 *Conceptualization of Top Managers' IT Security Awareness and Proposition Development*

Altogether, our literature research showed that research on IT security awareness at the top management level is rare. The extant literature focuses mainly on the impact of top managers' IT security awareness on the effectiveness of IT security management. Only a few studies analyze factors that determine top managers' IT security awareness. Moreover, these studies tend to focus on either individual-related or organization-related factors.

In the following, we first analyze top managers' IT security awareness by identifying the relevant factors that previous research has indicated. Then we focus on the concept of top managers' IT security awareness by investigating its role in organizational IT security management.

##### 4.2.3.1 Factors of Top Managers' IT Security Awareness

Only three papers in the final set were found to address factors that are relevant to top managers' IT security awareness (Isomäki and Bilozarov 2012; Ng and Feng 2006; Siponen 2001). Overall, the analysis of the identified literature indicates that top managers' IT security awareness is based on two dimensions: the individual and the organizational dimension. The individual dimension is determined by factors that result from top managers' personal environment and personal characteristics (e.g., Albrechtsen and Hovden 2010; Isomäki and Bilozarov 2012; Siponen 2000a). For example, top managers' individual knowledge about IT security threats and IT security controls or top managers' personal trust in IT security specialists are factors ascribed to the individual dimension of top managers' IT security awareness (see e.g., Isomäki and Bilozarov 2012; Ng and Feng 2006). Contrary, the organizational dimension of top managers' IT security awareness is determined by factors that result from the organization-specific environment such as the industry-specific sensitivity of an organization's data and IT systems to IT security threats or the organization-specific IT security environment as a result of an organization's previous investments in its IT security (e.g., Ng and Feng 2006; Straub and Welke 1998).

Siponen (2001) identifies five dimensions of general IT security awareness (organizational, general public, socio-political, computer ethical, and institutional education dimensions) whereas only the organizational dimension was found to apply to top managers. Within the organizational dimension the author argues that the members of different hierarchical levels (i.e., top management, IT management, IT security staff, computing/IT professionals, end-

users of various kinds, and third parties) need different kinds of knowledge about IT security to build an appropriate IT security awareness and that only sufficient knowledge about IT security risks and controls will enable them to fulfill their responsibilities with regard to the organizational IT security management.

Isomäki and Bilozarov (2012) conducted a literature review focusing in the first step on factors of IT security awareness at the top management level. They analyzed the most commonly used IT security awareness definitions at the employee level and extracted their factors. They found that two main factors (knowledge and behavior) were covered by all definitions. Drawing on the work of other authors, they also included attitude and motivation as factors of IT security awareness. In the second step, they used the four identified factors (i.e., knowledge, behavior, attitude, and motivation) for further investigations of top managers' IT security awareness. They conducted 19 semi-structured interviews with managers of small and medium-sized Northwest Russian enterprises and used a grounded theory approach to conceptualize the properties of the four individual factors of IT security awareness at the top management level. Other studies demonstrate that attitude and behavior are predominately associated with managerial and employee actions toward IT security (e.g., Bulgurcu et al. 2010; Choi et al. 2006; Choi et al. 2008). For example, Bulgurcu et al. (2010) argue that IT security awareness influences attitudes toward IT security and, eventually, behavior. In our study, we focus on the factors of top managers' IT security awareness that influence their IT security behavior regarding the organizational IT security management. Specifically, we analyze the influence of top managers' IT security awareness on top managers' decisions about IT security specialists' scope for action (e.g., IT security budget allocation). Therefore, in line with Bulgurcu et al. (2010) and Choi et al. (2008)<sup>2</sup> we consider attitude and behavior to be descendants of managerial IT security awareness and thus not factors of the individual dimension of top managers' IT security awareness. Based on the findings of related research (e.g., Albrechtsen and Hovden 2010; Siponen 2000a), we agree with Isomäki and Bilozarov (2012) that IT security knowledge and motivation are factors within the individual dimension of managerial IT security awareness. IT security knowledge can be seen as a precondition for understanding IT security risks. Individual motivation, which is also emphasized by Siponen (2000a), concerns issues that stimulate top managers to prioritize IT security issues (Isomäki and Bilozarov 2012). For example, top managers'

---

<sup>2</sup>

The studies by Choi et al. (2006) and Choi et al. (2008) are based on the same data, first published in *Proceedings of the Americas Conference on Information Systems 2006* and two years later as an extended version in the journal *Information Management & Computer Security*.

motivation covers the alignment between IT security and business needs (Ng and Feng 2006). Specifically, top managers are usually more motivated to invest in IT security when these IT security investments support the achievement of business goals. Furthermore, Ng and Feng (2006) identify top managers' trust in employees as a further factor of top managers' IT security awareness. Accordingly, trust in the IT security specialists is also assumed to constitute a factor within the individual dimension of top managers' IT security awareness. For example, if top management trusts the IT security specialists, the top management will be more likely to support the specialists' decisions, thus giving the IT security specialists a larger scope for action. Altogether, regarding the individual dimension of top managers' IT security awareness we propose:

*Proposition 1 (P1):* The individual dimension of top managers' IT security awareness is determined by top managers' individual IT security knowledge, their personal prioritization of IT security, and their trust in IT security specialists.

According to Choi et al. (2008), top managers' perceptions regarding IT security issues in the organization-specific environment are also relevant for their IT security awareness. For example, even if top managers have sufficient IT security knowledge and are generally motivated to protect the organizational IT systems, they might still perceive IT security risks as not relevant for their organization because they do not perceive their organization's data and IT systems to be attractive to attackers. Accordingly, top managers' evaluation of the industry-specific sensitivity of their organizations' data and IT systems is identified to be an organization-related factor of managerial IT security awareness. Moreover, several studies indicate the evaluation of the present IT security environment of an organization to be a further relevant factor of top managers' IT security awareness. As such, this factor reflects the organization-specific conditions of the IT systems. For example, it covers the effort that has been already taken to increase the IT security level of the organization (Choi et al. 2008; Goodhue and Straub 1991; Straub and Welke 1998). Consequently, we identify two factors within the organizational dimension of top managers' IT security awareness and propose:

*Proposition 2 (P2):* The organizational dimension of top managers' IT security awareness is determined by the industry-specific sensitivity of data and IT systems and the current IT security environment within the organization.

The definitions of the factors that are proposed to determine the individual and organizational dimension of top managers' IT security awareness (P1 and P2) are summarized in Table 9.

**Table 9: Factors of Top Managers' IT Security Awareness**

Dimension	Factor	Definition	References
Individual Dimension (P1)	Individual IT Security Knowledge	A top manager's general knowledge about IT security threats and IT security controls.	Isomäki and Bilozarov (2012); Siponen (2001)
	Personal Prioritization of IT Security	A top manager's personal motivation to increase the IT security level of the organization.	Isomäki and Bilozarov (2012); Ng and Feng (2006)
	Trust in IT Security Specialists	The extent to which a top manager believes the IT security specialists are honest, capable, and helpful in effectively protecting the organization's data and IT systems.	Ng and Feng (2006); Rustagi et al. (2008)
Organizational Dimension (P2)	Industry-Specific Sensitivity of Data and IT Systems	A top manager's evaluation of the industry-specific sensitivity of the organizations data and IT systems.	Choi et al. (2008); Goodhue and Straub (1991); Ng and Feng (2006); Straub and Welke (1998)
	IT Security Environment	A top manager's evaluation of the current IT security level in the organization.	Choi et al. (2008); Goodhue and Straub (1991); Ng and Feng (2006); Straub and Welke (1998)

#### 4.2.3.2 The Role of Top Managers' IT Security Awareness in the Organizational IT Security Management

Most of the 16 papers in the final set focus on the role of top managers' IT security awareness in organizational IT security management. These studies reveal that IT security awareness of top managers is critical to the effectiveness of IT security management (e.g., Boni 2000; Goodhue and Straub 1991; Rhee et al. 2012). For example, Wang and Hsu (2010) argue that top managers' IT security awareness not only influences IT security awareness at the employee level but also directly influences the organizational integration of IT security management. Specifically, IT security specialists' scope for action and thus, their ability to implement all necessary IT security controls strongly depends on the IT security awareness at

the top management level, which in turn influences the effectiveness of the organizational IT security management (e.g., Dang and Nkhoma 2013; Goodhue and Straub 1991; Wu and Saunders 2005). Choi et al. (2008) analyze the influence of top managers' IT security awareness on their actions toward IT security (e.g., development of IT security policies and procedures). The study shows that the effectiveness of IT security management within an organization strongly depends on the top managers' IT security awareness. Accordingly, the authors reveal that raising IT security awareness at the top management level should be an organization's priority in order to ensure effective IT security management. In this context, they are the first to provide evidence that supports the relationship between top managers' IT security awareness and managerial actions toward IT security. Moreover, Kajava et al. (2007) study the role that top managers' IT security awareness has in the process of implementing an IT security culture in the organization. The authors argue that top managers often assess IT security as a prerequisite for business success but do not have sufficient IT security knowledge for ensuring effective IT security management. They state that raising the top management's IT security awareness will positively influence the effectiveness of IT security management because IT security-aware top managers will take more effective IT security measures. As such, a top-down effect from the management level to the employee level is proposed (e.g., Kritzinger and Smith 2008). Numerous studies have investigated the success of IT security measures at the employee level and thus, the protection of the entire organization (e.g., Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009a; Vance et al. 2012).

Overall, researchers argue that the relation between top managers and IT security specialists is particularly important (e.g., Forte 2008; Mouratidis et al. 2008). IT security awareness at the top management level determines top management's strategic decisions and consequently the IT security specialists' scope for action (i.e., the organizational integration of IT security management) (Cline and Jensen 2004). In particular, only sufficient IT security awareness at the top management level will ensure a focus on IT security within the organization's strategy. Especially in cases of conflicting objectives, attracting top management support for the organization's IT security management is crucial (e.g., Dutta and McCrohan 2002; Johnson and Goetz 2007; Knapp et al. 2006; Narain Singh et al. 2014). For example, if the top management does not have sufficient IT security awareness, they are more likely to focus on business-driven investments than on investments in their organizations' IT security and thus will not allocate sufficient resources and flexibility in IT security-related decision-making to



the organizations' IT security specialists. Accordingly, top managers' IT security awareness is proposed to increase the IT security specialists' scope for action. Therefore, we propose:

*Proposition 3 (P3):* Top managers' IT security awareness positively affects the scope for action of IT security specialists.

By definition, the IT security specialists' scope for action strongly influences the effectiveness of the organizational IT security management (e.g., Dang and Nkhoma 2013; Goodhue and Straub 1991; Wu and Saunders 2005). In particular, the IT security specialists can only ensure an appropriate level of IT security within the organizations when they have the necessary budget to build the required resources (Workman et al. 2008). Therefore, we further propose:

*Proposition 4 (P4):* The scope for action of IT security specialists positively affects the IT security level of an organization.

The developed conceptualization of top managers' IT security awareness after Step 1 of this study (literature review) can be extracted from Figure 8 (see page 65).

### **4.3 Step 2: Evaluation of the Conceptualization of Top Managers' IT Security Awareness**

In this section, we present an evaluation of the developed conceptualization of top managers' IT security awareness.

#### *4.3.1 Research Approach*

We conducted qualitative expert interviews to evaluate the factors identified in the previous sections within the individual and organizational dimensions of top managers' IT security awareness, to identify additional factors of top managers' IT security awareness, and to evaluate its role in the organizational IT security management.

On the one hand, we interviewed IT security experts at different hierarchical levels of a European organization and on the other hand IT security suppliers. Interviewing different parties responsible for the IT security management in a large organization allowed us to cover different perspectives on top managers' IT security awareness and its role in organizational IT security management from different hierarchical levels. Moreover, interviewing IT security suppliers enabled us to benefit from their wide-ranging experiences with the IT security management in several organizations.

**Table 10: Descriptive Information for Interviewed Experts**

Ex- pert	Position	Company Size (No. of Employees)	Sales p.a.	Industry
#1	CISO	Large (>249)	> 99 m EUR	Transportation
#2	IT security manager (policies & compliance)			
#3	IT security director (cyber defense)			
#4	IT security manager (department level)			
#5	CEO	Small (<50)	1-9 m EUR	IT security products and services
#6	Product manager	Large (>249)	10-99 m EUR	
#7	IT security auditor	Large (>249)	> 99 m EUR	

In total, seven semi-structured interviews with a total duration of 10 hours and 28 minutes were fully transcribed and coded by the authors of this paper (three IS researchers). Descriptive information about the interviewed experts is given in Table 10. The structure and guiding questions of interviews with the different participants (IT security experts in the organization and IT security suppliers) are presented in Table 11.

**Table 11: Structure of Interviews**

Participants		
Structure of Interviews	IT Security Experts in Organization	IT Security Suppliers
	1. Profile of participant and organization	1. Profile of participant and organization
	2. Definitions	2. Definitions
	3. Guiding questions: <ul style="list-style-type: none"> <li>How are decision-processes in the IT security management of your organization designed?</li> <li>How would you describe the IT security awareness of top managers and its role in organizational IT security management?</li> </ul>	3. Guiding questions: <p><i>Based on your experiences with customer organizations, ...</i></p> <ul style="list-style-type: none"> <li>How are decision-processes in the IT security management designed?</li> <li>How would you describe the IT security awareness of top managers and its role in organizational IT security management?</li> </ul>
	4. Further comments and conclusion	4. Further comments and conclusion

### 4.3.2 Qualitative Data Analysis

For initial coding of the data, we decided to apply an exploratory coding method since these methods permit open-ended investigation (Saldaña 2015). Specifically, within the first coding cycle we chose *provisional coding* (see also Dey 2003; Miles and Huberman 1994). The corresponding provisional list of codes is generated from the results of the literature review as suggested by Saldaña (2015). Thus, we use our conceptualization of top managers' IT security awareness developed in Step 1 of this study (propositions P1-P4) as the coding framework and accordingly focused on the individual and organizational factors determining top managers' IT security awareness as well as on the role of top managers' IT security awareness in IT security management.

For the second coding cycle, we chose *focused coding* which is appropriate for almost all qualitative studies and particularly for developing major categories from the data and developing new theory about a phenomenon (Charmaz 2014; Saldaña 2015). The two coding cycles resulted in three coding categories, as shown in Table 12. The codes within each of the categories are explained in the following sections.

**Table 12: Coding Categories**

<b>Coding Categories</b>	<b>Number of Codes</b>
<i>Individual dimension of top managers' IT security awareness (P1)</i>	67
<i>Organizational dimension of top managers' IT security awareness (P2)</i>	39
<i>Role of top managers' IT security awareness in IT security management (P3, P4)</i>	37

#### 4.3.2.1 Factors of Top Managers' IT Security Awareness

Our results show that the three factors — the individual IT security knowledge and the personal prioritization of IT security of top managers as well as their trust in IT security specialists — determine the individual dimension of IT security awareness at the top management level, as proposed in P1. All experts confirmed that top managers need a certain degree of *individual IT security knowledge* to be able to understand the necessity of IT security in the organizational IT systems. They emphasized that a lack of IT security knowledge is one of the main obstacles regarding top managers' IT security awareness. Moreover, expert #1 stated that often, top managers do not even try to understand the issue. Therefore, it is even more difficult for IT security specialists to explain the necessity and

benefits of IT security risk reduction (e.g., prevention of customer loss or reputational image): “People think IT security is a highly complex topic that one simply cannot understand. That is why it is often so difficult for us to explain the benefit we want to generate with that investment [...] and to explain the topic to the management board” (#1).

Regarding the *personal prioritization of IT security* within the individual dimension of top managers' IT security awareness, the results show that this individual IT security awareness factor strongly depends on conflicting objectives. These conflicting objectives are perceived to be mainly due to the tension between IT security, usability, and costs (“It is always a trade-off between IT security, usability, and costs”, #3). While IT security specialists' main objective is to effectively protect the organization from IT security risks, top managers tend to be more business-oriented (i.e., usability- and cost-oriented): “IT security investments are always in competition with other IT investments [...] which are seen to be more useful and valuable from the business perspective” (#1). Conflicting objectives, not only between the top management level and IT security specialists but also between department managers and IT security specialists, were highlighted by the experts. A primary objective of department managers is ensuring smooth, fast processes for attaining business objectives. Consequently, they often perceive IT security as a barrier that slows down business processes and requires high investments while there is neither an obvious return on the investment nor a visible effect: “[The departments] have to reach their business goals. And the most important objective is that people can do their work [...]. [Most of them] perceive IT security as a barrier and just want to attain their business goals” (#5); “And when they invest a million no one sees anything [...], because the IT security specialists are blocking it. And then they ask: For what am I spending money? I never hear anything” (#4); “They normally could invest the money in business goals. Why should they spend it on this expensive thing called IT security?” (#3); “As a result, [...] IT security is actually never requested” (#1).

The potential for conflicting objectives between top management, IT security specialists, and department management was summarized by expert #6: “The top management is focused on investments with benefit. [...] The IT security specialists always want to have the most secure solution, which is usually also the most expensive. [...] And since IT security is always associated with a reduction in the ease of system use, you will always encounter resistance from the department level”.

In sum, personal prioritization of IT security was found to be a relevant factor of the individual dimension of top managers' IT security awareness, strengthening support for P1.

The higher a top manager's priority of IT security, the higher the individual dimension of managerial IT security awareness. Expert #3 stated that the source of the individual motivation of top managers toward IT security is crucial: "Is it important to him because it protects him personally in terms of his personal liability as a board member? Or is it important to him because he believes that he will ensure the survival of the company [...] or because he knows that he must be compliant [...] due to regulatory reasons?"

Regarding the *trust of top managers in IT security specialists*, the experts often mentioned that top managers frequently do not trust the recommendations of their own IT security specialists and therefore demand a second opinion: "The top management would more likely listen to an IT security specialist of another organization than to its own" (#4). Expert #5 explained that he already had the experience that top managers got angry when IT security specialists disclosed essential new IT security risks to them and, moreover, that sometimes they would not even trust the opinion of a second specialist: "Most of our clients calm down when a second opinion is available. But we have also encountered situations where a second opinion did not matter".

Furthermore, our study identified not only IT security knowledge, personal prioritization of IT security, and trust in IT security specialists as factors determining the individual dimension of top managers' IT security awareness, but also top managers' *individual experience with IT security incidents* ("The awareness is always as great as the pain you have experienced", #1), extending P1. Expert #5 mentioned that organizations predominately react in a passive manner in the context of IT security: "If the phone rings and someone says: 'We want to talk about security'. Then you can be sure that something already happened. [...] No organization handles that really proactively". Expert #6 also acknowledged this: "In my experience, many organizations do not even look at IT security seriously, and so they do not even realize that it can be serious. And most of the organizations only react when something has already happened". Additionally, the experts argued that top managers also show a higher level of IT security awareness when they observe IT security incidents in other organizations that have resulted in financial and reputational damage. Accordingly, when top managers' IT security awareness is higher due to a recent IT security incident, IT security specialists have better chances to implement the corresponding IT security safeguards: "What we have learned in the past [...] is that [we can use] large security incidents [in other organizations] for our own goals. Always, when something has just happened we have [...] higher [management] attention" (#2).

Moreover, we found that individual experiences with IT security incidents in both working life and private life increase the level of the individual dimension of managerial IT security awareness: “If he has just been a victim — he has just been hacked in his private life or the organization has just lost large databases and has suffered reputational damage — both can be just as beneficial [from the IT security specialists’ perspective]” (#3).

Regarding the organizational dimension of top managers’ IT security awareness, the results of our study also strengthen support for P2. The experts argued that the organizational dimension of top managers’ IT security awareness strongly depends on the *perceived industry-specific sensitivity of data and IT systems*, i.e., the evaluation of IT security risks that organizations face in terms of their industrial environment. The experts stated that in organizations that operate in industries where research and development activities are essential, which raises the risk of industrial espionage, top managers tend to show a higher level of managerial IT security awareness. As an example, the automotive and the pharma industries were mentioned multiple times. Within these industries, very sensitive data is processed and stored by organizations’ IT systems, e.g., blueprints of a new car: “For example, in the automotive industry. The development of a car costs a few billion Euros. And therefore, they make it more secure” (#4).

Moreover, the *perceived IT security environment* at present was also evaluated by the experts to be a relevant factor in the organizational dimension of top managers’ IT security awareness. In this context, while the relevance to the business model was found to increase the level of top managers’ IT security awareness, previous investments to ensure the IT security of the organizational IT systems show a decreasing effect on the organizational-dimension of top managers’ IT security awareness: “But you can actually assume that when organizations operate with critical personal information, such as credit card information, these organizations are investing significantly more [in IT security] because their business model is based on this data. For example, if it were to become public that Amazon has lost all customer data and that it was not encrypted, they may have to close their store” (#6). Expert #7 stated: “And then top managers ask why the IT security specialists still want to have a larger budget. They have already invested so much money and effort to achieve a more secure situation”.

In addition to the *perceived industry-specific sensitivity of data and IT systems* and the *perceived IT security environment* of the organization, *legal requirements* (e.g., compliance guidelines in the financial sector) were often mentioned as a factor within the organizational dimension of top managers’ IT security awareness: “Changes in legal requirements [...] will

always have the strongest impact on top managers' IT security decision-making" (#7). This indicates that P2 has to be extended by the addition of legal requirements as a factor of the organizational dimension of managerial IT security awareness. Nevertheless, even though legal requirements were often mentioned by the experts, our findings also show that their effect on managerial IT security awareness is doubted to some extent. Expert #1 stated that the actual fulfillment of legal requirements in an organization is situation specific ("The status of compliance varies a lot", #1). Expert #5 further explained: "At the moment, we have that huge question in the banking sector. They only meet the legal requirements. [...] They check legal requirements with the help of a lawyer. [...] And try to meet the relevant legal requirements at the lowest possible costs. They do not care if the measures they take make any sense or are effective. And I can say that in many cases, the top management only employs a CISO [...] because of legal regulations".

#### 4.3.2.2 The Role of Top Managers' IT Security Awareness in the Organizational IT Security Management

Our results show that the contrary distribution of IT security knowledge and decision power across the different hierarchical levels of an organization is often perceived to inhibit the effectiveness of the organizational IT security management. While top management often shows a lack of IT security knowledge, the IT security specialists at the department level usually have better knowledge concerning IT security yet their scope for action is restricted by the top management. The experts emphasized that effective IT security management needs both IT security knowledge ("Decision makers need a fundamental understanding of IT security issues for ensuring effective IT security management", #1) and the corresponding decision power ("The problem is that the final decisions are usually made at the top management level", #6). For example, expert #5 stated: "When we only talk to the technical staff, we do not get far, because the budget is controlled by the top management" (#5). Expert #6 observed that even if "the IT security specialists have good ideas [...], there is no one in the top management who understands these issues [...]". Expert #7 argued that "even in the early planning phase for IT security strategies and goals, IT security specialists are for the most part not included or not taken seriously in the discussions". Furthermore, expert #5 highlighted that an organization's IT security management is characterized by "a lot of politics. There are many political dependencies within the organization, but there is often a low level of common sense among managers". Accordingly, expert #6 stated that to ensure effective IT security awareness, an IT security specialist with relevant knowledge about IT

security should be positioned in the top management: “Particularly because [...] decisions are finally made in the top management, an appropriate position must be represented in and heard by the top management”. It was argued that positioning IT security specialists in the top management is the key for “making the issue and its dimensions understandable at the top management level and for achieving acceptance in the organization” (#6). This was also confirmed by expert #1: “A position that has decision power and IT security knowledge at the same time would be a critical success factor for effective IT security management”. In sum, our results show that in order to ensure IT security in an organization, IT security specialists need a certain scope for action which is ultimately determined by top managers' IT security awareness, thus supporting P3. A higher level of top managers' IT security awareness will positively influence the scope for action of IT security specialists within an organization.

Specifically, the experts mentioned three main problems regarding IT security specialists' scope for action that inhibit effective IT security management: budget restrictions, restricted human resources, and lack of flexibility. Expert #2 highlighted the challenge of *budget restrictions*: “I think that in 80 to 90 percent of the cases, the budget is the reason for a decision against an IT security investment”. Expert #1 mentioned that although an IT security safeguard had already been proven to be necessary and effective, the top management did not perceive the necessity of its implementation and accordingly, did not allocate the budget for the investment: “I did not get the money for the implementation until now because the mechanisms in the organization prevented that”. Not only budget restrictions but also *restrictions regarding human resources* are often perceived to restrict IT security specialists' scope for action and thus, to further inhibit IT security specialists to increase the organization's IT security level: “We assume that you also need a basis of human resources. But currently we do not have enough IT security specialists in our organization. Or at least they are not employed full-time for performing IT security management tasks, because that would mean a permanent [...] resource commitment in our organization” (#1). Many decision makers in the participating organizations mentioned that another major inhibitor for ensuring a high level of IT security is *restricted flexibility* in the decision-making of IT security specialists. The experts stated that IT security investments have to compete with other IT investments in their organization. As a result, decisions about IT security investments have to “go through a process that you cannot really accelerate. This decreases the flexibility of the IT security specialists [...] and sometimes it takes two, three, or more years until they achieve something” (#3). Expert #7 concluded that IT security specialists need a certain degree of flexibility, or at least “easy and direct communication between IT security specialists and

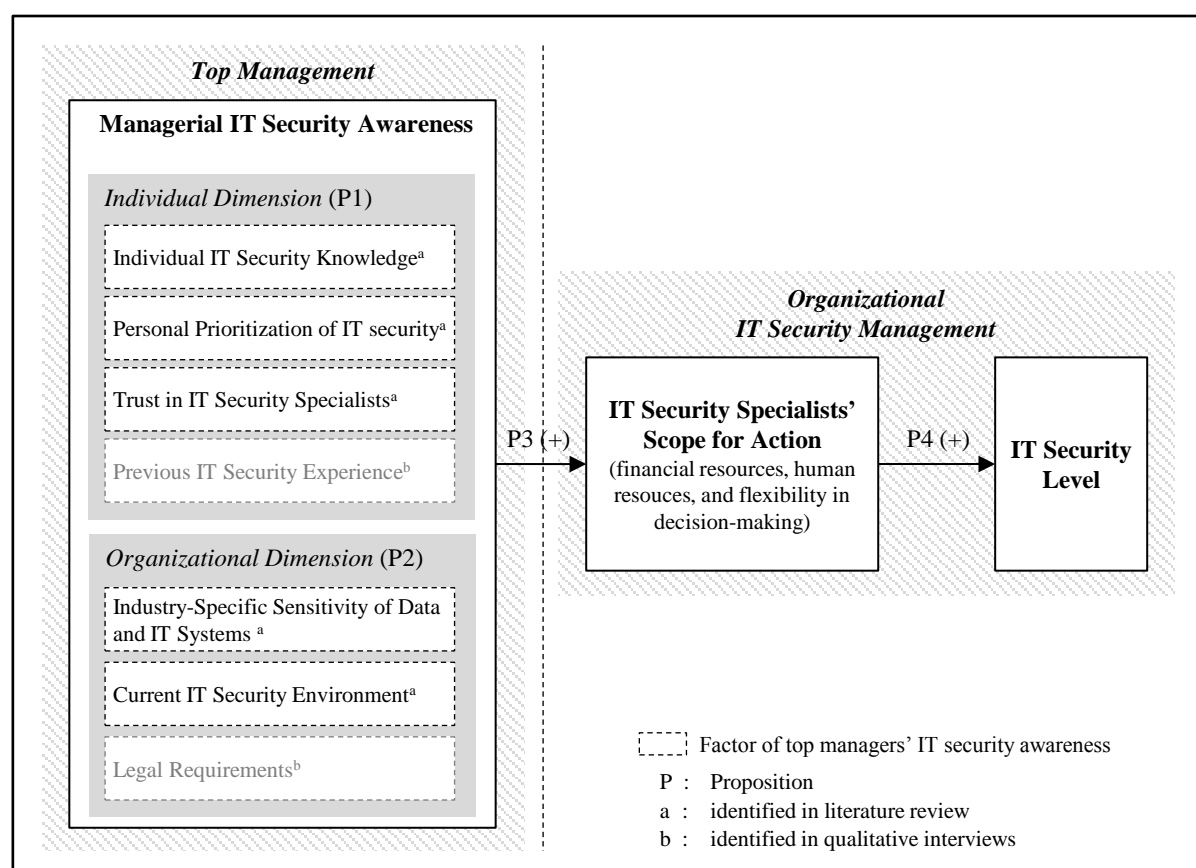


decision makers". The flexibility of IT security specialists becomes even more important when the dynamic nature of IT security due to the fast technological developments (i.e., new IT security threats arise) is considered. Especially in situations that require timely decisions to ensure protection of the organization against IT security risks, IT security specialists need to have a certain degree of flexibility: "Identifying a new IT security risk means that there is a new threat to our organization and therefore, we have to be prepared as quickly as possible" (#3).

Our findings strengthen the support for P4 by confirming that IT security specialists' scope for action positively influences the effectiveness of the organizational IT security management and thus, the IT security level of an organization. In addition, our results show that this scope for action is primarily restricted by resources, including financial resources (i.e., IT security budgets), human resources (i.e., the number of full-time employed IT security specialists), and the degree of flexibility in decision-making (i.e., dependence on decisions made by top managers).

Moreover, our results point out that not only managerial IT security awareness at the top management level determines IT security specialists' scope for action but also the managerial IT security awareness of department managers: "And there are five departments that have to share the costs for the IT security safeguard implementation. Maybe two or three of them will assess the IT security investment as positive, but [...] there will be other departments whose managers say 'No, that is too expensive for us'" (#2); and if "the CISO is integrated in the IT department, he cannot do anything about it, because he cannot tell these departments to make certain investments" (#7). In line with P4, not only is "the IT security awareness of top managers [...] a key success factor for effective IT security management" (#1), but also the IT security awareness of the department managers. Accordingly, IT security specialists' scope for action was confirmed to depend on managerial IT security awareness at both the top management level and the department level.

Altogether, the evaluation of the proposed conceptualization revealed that top managers' IT security awareness has both an individual and an organizational dimension (P1 and P2). The results also confirm that a high level of managerial IT security awareness positively influences IT security specialists' scope for action (P3) and that an appropriate scope for action of IT security specialists (financial resources, human resources, and flexibility in decision-making) in turn, positively influences the IT security level of an organization (P4). The resulting conceptualization is shown in Figure 8.



**Figure 8: Conceptualization of Top Managers' IT Security Awareness**

To further confirm the validity of the initial clustering of the identified factors within the individual and organizational dimension, we additionally applied a Q-sort method (Thomas and Watson 2002) as a final step in our evaluation of the developed conceptualization of top managers' IT security awareness. Q-sorting is "a modified rank-ordering procedure in which stimuli are placed in an order that is significant from the standpoint of a person operating under specified conditions" (Brown 1986). In total, eight IS researchers in IT security and privacy participated in the Q-sort. First they were presented with short definitions of the identified factors. Then, they were asked to assign the factors identified within the literature review and expert interviews to the two dimensions of top managers' IT security awareness. As the method allows marking factors that do not fit to any dimension, it can also eliminate factors that are not a part of top managers' IT security awareness. However, none of the factors were perceived by the IT security experts to not fit the construct. Afterwards, we calculated interrater reliability metrics to assess the validity of the categorization (Moore and Benbasat 1991). In this regard, an average Fleiss Kappa value of 0.63 and an average dimension hit ratio of 0.89 point to a high degree of validity (Landis and Koch 1977). In sum, the results of the Q-sorting confirm that the individual dimension of top managers' IT security awareness is determined by the following four factors: top managers' IT security knowledge,

personal prioritization of IT security, trust in IT security specialists, and previous IT security experience (extended P1). Three factors were found to belong to the organizational dimension of top managers' IT security awareness: industry-specific sensitivity of data and IT systems, the IT security environment, and legal requirements (extended P2).

#### **4.4 Discussion**

Our literature review revealed that only a few studies analyze the conceptualization of IT security awareness at the top management level in organizations. In the first step, we developed a conceptualization of top managers' IT security awareness. Therefore, we identified the relevant factors and analyzed how they determine the individual and organizational dimensions of top managers' IT security awareness. Specifically, we found in the extant literature that top managers' individual IT security knowledge, their personal prioritization of IT security, and trust in IT security specialists determine the individual dimension, whereas the perceived industry-specific sensitivity of an organization's data and IT systems and the evaluation of the current IT security environment determine the organizational dimension. In the second step, we evaluated the proposed conceptualization with qualitative expert interviews and Q-sorting. This led to the confirmation of previously identified factors and moreover, revealed two additional factors that have been overlooked by previous studies identified in our literature review but are relevant to top managers' IT security awareness: previous IT security experience and legal requirements. While the IT security experience (individual dimension) has an apparent positive effect on managerial IT security awareness, industry-specific legal requirements (organizational dimension) were assessed to only have a marginal effect in certain situations. In particular, it has been emphasized by the IT security experts that top managers often try to fulfill mandatory legal requirements at the lowest possible cost and consequently do not effectively address IT security risks.

Additionally, we analyzed the role of top managers' IT security awareness for the effectiveness of the organizational IT security management. Even though the IT security specialists are generally more focused on ensuring a high level of IT security in the organization, their scope for action is oftentimes too restricted by top management. Specifically, we found that the scope for action of IT security specialists is restricted by financial resources (i.e., IT security budgets), human resources (i.e., the number of full-time employed IT security specialists), and the degree of flexibility in decision-making (i.e., dependence on decisions made by top managers). For example, IT security specialists might

be aware of a specific IT security risk and thus recommend the implementation of a certain IT security measure to the top management level. If top managers do not take this IT security risk seriously, they will not allocate the necessary budget or additional human resources. Additionally, dependent on the organizational size, not only IT security awareness of top managers can be crucial to the effectiveness of IT security management, but also the IT security awareness of managers at the department level. If department managers are involved in organizational decision-making regarding IT security management (e.g., participation in IT security budget allocation), they also need to have an appropriate level of managerial IT security awareness. For example, if an IT security investment incurs running costs or additional efforts for departments individually, these departments will only support the IT security investment with the relevant managerial IT security awareness at hand.

This paper provides three theoretical contributions. First, our study makes important theoretical contributions by developing and evaluating an exhaustive conceptualization of managerial IT security awareness at the top management level including both individual- as well as organization-related factors. Second, this work shows that not only top managers' IT security awareness but also department managers' IT security awareness is relevant for an effective IT security management. Thus, we highlight the importance to consider all hierarchical levels of an organization when studying IT security management. Third, our study contributes to the emerging body of IT security awareness literature by highlighting and confirming the important role of managerial IT security awareness for an effective IT security management in organizations.

In addition, this paper provides important contributions for practitioners. It shows that the effectiveness of organizational IT security management strongly depends on the managerial IT security awareness of decision makers at both the top management and the department levels. The IT security level of the entire organization can only be increased when managers throughout the entire organization are aware of IT security and their important roles in establishing effective IT security. Consequently, organizations should not only focus on IT security awareness at the employee level but also on the IT security awareness of all managers in the organization. Our findings emphasize that the combination of decision-making power (i.e., scope for action) and IT security knowledge is crucial for effective IT security management. Specifically, specialists responsible for the IT security in the organization need — apart from the required IT security knowledge — sufficient financial resources, human resources, and the necessary degree of flexibility in decision-making for

effectively protecting an organization's IT systems. Thus, organizations should identify and integrate appropriate positions in their organizational structure to increase their overall IT security level. For example, in order to increase managers' trust in IT security specialists, organizations need to adjust the organizational integration of the IT security management assuring a direct communication between involved parties. Additionally, the IT security specialists should provide regular management reports about current IT security threats for their organizations on an abstract and non-technical level. In doing so, top managers can easily gain knowledge about IT security issues and realize the necessity of certain IT security investments. In this context, round-table discussions between managers and IT security specialists could be used to ensure a balanced discussion of the organizations' IT security needs in view of the business objectives.

#### **4.5 Limitations and Future Research**

The aim of this study was to improve our understanding of top managers' IT security awareness by developing and evaluating an exhaustive conceptualization of managerial IT security awareness including both individual- as well as organization-related factors. With a better understanding of these factors, this work provides a basis for future research to better understand the formation of organizational IT security investment decisions. In particular, results from previous studies indicate that although managers might show concern regarding the IT security of their organizational IT systems, their stated attitudes may not be in accordance with their actual IT security behavior (i.e., low IT security investments). Taking the results from this study into account, the conceptualization of top managers' IT security awareness may enable future research to explain this paradoxical attitude-behavior gap. Additionally, understanding the factors determining managers' IT security awareness enables researchers to develop and empirically test dedicated measures to improve managers' IT security awareness (e.g., awareness trainings particularly designed for managers, or security incident event management tools or systems of IT security indicators aligned to the needed managerial IT security awareness), and thus increase the effectiveness of the organizational IT security management.

Nevertheless, four limitations of this paper merit consideration. First, the developed conceptualization in this paper is only a starting point in research about top managers' IT security awareness. Without a doubt, further studies that evaluate the proposed conceptualization of top managers' IT security awareness are needed. Future research can enrich the results of this paper by testing the proposed conceptualization of top managers' IT

security awareness and the influence of its dimensions in a large-scale empirical study. Moreover, while our results highlight the importance of considering all hierarchical levels of an organization when studying IT security management, only four managers in one organization and three IT security suppliers were interviewed during Step 2 of our study. These experts might have their own and thus biased security-related views, values, and goals. Therefore, future research should conduct additional interviews with all managers that participate in the organizational IT security management — including CEOs, CISOs, CIOs, and department managers — within different organizations of various industries. These studies should also analyze to what degree the identified factors of managers' IT security awareness are different and similar among different industries. Beyond that, additional research is needed regarding the influence of managerial IT security awareness at different management levels (i.e., top management and department management) on IT security specialists' scope for action as well as the effectiveness of the IT security management. By using the results of this study as a starting point and further validating the results, future research can better understand and address potential areas of conflict between different organizational levels in the context of IT security investment decisions. Second, the proposed conceptualization of top managers' IT security awareness is rather generic. In particular, the organizational structure of small organizations may differ from the organizational structure presented in this paper (e.g., the CEO may also be directly involved in IT security management). Small organizations may have less IT security knowledge (Kotulic and Clark 2004) because larger organizations can employ more IT security specialists (Hoffer and Straub 1994) and allocate more resources for IT security. Hence, future research can add to the findings of our study by investigating the effects of firm size and different organizational structures on managerial IT security awareness. Third, the study was conducted in a European country. The experts mentioned that they perceive organizations in the U.S. to be more aware of IT security. Accordingly, future studies should also consider international differences. Fourth, this study assumes that IT security specialists possess an adequate knowledge about IT security risks and measures to make proper decisions for ensuring an appropriate level of IT security. Future research can enrich the findings of this study by investigating the decision-processes and the organizational integration of IT security management in order to assess the actual quality of decisions concerning the organizational IT security.

## 4.6 Conclusion

Overall, this paper advances our understanding about the role of top managers' IT security awareness in organizational IT security management and provides several theoretical and practical implications. By developing and evaluating an exhaustive conceptualization of managerial IT security awareness and by identifying two additional factors that have been disregarded by previous research, this work provides a basis for the emerging body of IT security awareness literature. Moreover, since the study revealed that not only the IT security awareness of top managers but also managers at the department level is crucial for effective IT security management, we highlight the need for considering all hierarchical levels of an organization when studying IT security management. Practitioners can learn that an effective IT security management is ensured by the combination of decision-making power (i.e., scope for action) and IT security knowledge. Without identifying and integrating appropriate positions in their organizational structure, organizations will be not able to maintain or (eventually) increase their overall IT security level. An organization that overlooks or ignores the impact of top managers' IT security awareness on the outcome of IT security management might pay a significant price when an IT security incident occurs. Such an IT security incident could have been prevented by sufficient awareness of the managers, resulting in an appropriate IT security management.

## 5 Research Paper C: Decision Makers' Willingness To Pay for IT Security

**Title:** Which IT Security Investments Will Pay Off for Suppliers? Using the Kano Model to Determine Customers' Willingness to Pay

**Authors:** Sonnenschein, Rabea  
Loske, André  
Buxmann, Peter

**Published in:** Proceedings of the 49<sup>th</sup> Annual Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii 2016

### Abstract

*Although cost-benefit analyses are an important aspect of information technology (IT) security management, previous research focuses largely on the customer perspective and neglects the supplier side. However, since ensuring a high level of IT security in modern IT products is typically associated with a large investment, customers' willingness to pay is essential for decision making in the context of IT product development. We draw on Kano's Theory of Attractive Quality to analyze how customers generally evaluate implemented IT security safeguards. Based on expert interviews and a large-scale empirical study involving customer company decision makers, this paper demonstrates that different customer evaluations of IT security safeguards are associated with different levels of willingness to pay. Therefore, our results will enable IT suppliers not only to understand their customers' IT security needs but also to derive optimal IT security strategies, which may provide both economic and competitive advantages. Further theoretical and practical implications are also discussed.*

**Keywords:** Customer Satisfaction, Companies, Security, Investment, Economics, Information Systems, Software Development, IT Security, Willingness to Pay, Kano.



## 5.1 Introduction

In the last few decades, the information technology (IT) needs of companies have grown tremendously. Recent technological advances and the Industry 4.0 paradigm are further leveraging this development. Due to the high complexity of modern IT systems, such as complex enterprise software, most of these are purchased from specialized supplier companies. However, the ubiquity of IT systems and the increasing interconnectedness of the resources entail constantly rising IT security risks. Recent studies reveal that customers are generally highly concerned about the security of their systems and data and therefore expect a high level of IT security, making it an important attribute of IT products and a possible competitive edge for suppliers (Lacity et al. 2009). Nevertheless, keeping IT security breaches down also requires suppliers to make larger investments for the development and implementation of effective IT security safeguards. Given the considerable increase in IT security effort, more and more suppliers face the question of whether their customers are actually willing — at least partially — to bear these costs, e.g., by paying a higher price for the product (Willcocks et al. 1996). As such, the trade-offs between risk and costs are relevant not only to customer organizations but are also essential for IT suppliers when making decisions about which safeguards to implement in their IT products. Although several studies address IT security at the organizational level (e.g., Goodhue and Straub 1991; Straub and Welke 1998), these studies focus only on perceptions of the absence of IT security (i.e., IT security risks) and largely neglect assessments of the presence of IT security (i.e., safeguards). Thus, little is understood about how customer companies evaluate the implementation of safeguards. Even more importantly, due to this knowledge gap, much uncertainty still exists about customers' willingness to pay (WTP) for IT security safeguards, which is eventually determined by their evaluations of the measures taken. This study seeks to provide data that will help address these research gaps.

We conducted expert interviews with customer company decision makers and draw data from a large-scale empirical study. By transferring Kano's Theory to the IT security context, we were able to shed light on the different evaluations of IT security safeguards made by customer companies. Safeguards typically have functional (e.g., prevention of unauthorized data access) as well as dysfunctional (e.g., reduced ease of system use due to requiring multiple passwords) characteristics. However, the weighing of the functional and dysfunctional characteristics of a safeguard may differ for different targeted customer groups. For example, some customers may utilize a suppliers' IT product to process sensitive data (e.g., personal and financial data) and thus assess the function of a particular safeguard as

indispensable. Other customers may not require the same level of IT security due to different IT security risk protection requirements and may therefore assess the safeguard as rather negative because of its dysfunctional characteristics. In addition to examining customers' evaluations of a safeguard's functional and dysfunctional characteristics, we show that these evaluations largely determine their WTP.

By enriching our understanding of how customer companies evaluate IT security safeguards, this study makes significant contributions to IS research. The study also offers theoretical explanations of and empirical support for the relationship between IT security safeguard evaluation and customers' WTP. Whereas previous IT security management research only focuses on the cost-benefit analyses made by customer organizations, this study adopts the perspective of suppliers and investigates the economic efficiency of providing security in IT products. Moreover, our results enable IT supplier firms to understand their targeted customers' IT security risk protection requirements so that they can develop optimal IT security strategies that may provide them with both economic and competitive advantages. Further theoretical and practical implications will also be discussed.

## **5.2 Theoretical Background and Research Hypotheses**

### *5.2.1 Kano's Theory of Attractive Quality*

In Kano's Theory of Attractive Quality (Kano et al. 1984), the presence of a certain product attribute does not necessarily imply a higher level of customer satisfaction. The theory postulates that the relationship between a product attribute and customer satisfaction generally depends on the customer's individual requirements (Matzler and Hinterhuber 1998). Accordingly, the theory considers both customer assessments of an attribute's functional characteristics (i.e., their response when a certain attribute is present in the product) and their assessments of the attribute's dysfunctional characteristics (i.e., their response when the attribute is absent). Based on these assessments, product attributes can be classified into five categories that meet different kinds of customer requirements and therefore influence customer satisfaction differently: basic, performance, advanced, indifferent, and reverse attributes (Kano et al. 1984; Matzler and Hinterhuber 1998).

Basic attributes are those that lead to dissatisfaction when they are absent but do not generate satisfaction when they are present. Basic attributes represent the minimal requirements for a customer. If these requirements are not fulfilled, the customer will not even consider the product. Therefore, basic attributes can be interpreted as a market entry "threshold" (Matzler

et al. 2004a). For example, airbags might be an attribute meeting the basic requirements for a car. The presence of a performance attribute leads to a proportional degree of satisfaction, and its absence leads to a proportional degree of dissatisfaction. For example, high gas mileage (low petrol consumption) might be a performance attribute for a car, and the higher the mileage, the greater the satisfaction (Matzler and Hinterhuber 1998; Tan and Shen 2000). Advanced attributes have the greatest influence on customer satisfaction but their absence does not lead to dissatisfaction, because customers do not expect these attributes to be present. Their presence delights customers and thus, according to Kano's Theory, advanced attributes have the greatest potential for differentiating a company's product from competitor products. For a car, a power rear view mirror might be an advanced product attribute (Tan and Shen 2000). In contrast, reverse attributes lead to dissatisfaction because the customer does not want them and expects them to be absent. As an example, the presence of rust spots on a car would produce dissatisfaction because the customer perceives this attribute to be dysfunctional. In the case of indifferent attributes, the customer does not care about the attribute's presence or absence. Thus, an indifferent attribute produces neither satisfaction nor dissatisfaction. For example, a sun roof might be an indifferent attribute for some customer groups.

Kano's Theory has been applied in several research fields, including product development projects (e.g., Matzler and Hinterhuber 1998; Tan and Shen 2000), management support systems (e.g., Mayer 2012), new (mobile) service creation (e.g., Bhattacharyya and Rahman 2004; Mette et al. 2013), website design (e.g., Gemmo et al. 2003; Zhao and Roy Dholakia 2009), internet community bonding (e.g., Szmigin and Reppel 2004), and e-services (e.g., Nilsson-Witell and Fundin 2005). Based on customer questionnaires, the theory helps supplier companies derive product development strategies, e.g., prioritizing development efforts and managing product development resources (Seder and Alhazza 2014). Since Kano's Theory provides insights into which different product attributes influence customer satisfaction and how, the model is also appropriate for investigating the influence of different product attributes on customers' WTP (e.g., Sakao 2009). The financial impact of customer satisfaction on supplier companies is well recognized (e.g., Ittner and Larcker 1998; Mittal et al. 2005). For instance, several studies in marketing research have already examined the relationship between customer satisfaction and customer WTP (e.g., Anderson 1996; Homburg et al. 2005).

In accordance with the U.S. National Institute of Standards and Technology, we define IT security as “a system characteristic and a set of mechanisms [...]” (Stoneburner et al. 2002). Consequently, the IT security safeguards (i.e., the set of IT security mechanisms) that are implemented in an IT system can be seen as different IT security attributes of the IT product. Recent research already recognizes that IT security safeguards are not only perceived as functional (e.g., reducing risks) but also as dysfunctional (e.g., reducing the usability of the IT system). For instance, there is a separate research stream that emphasizes the negative consequences of poor usability resulting from security mechanisms (e.g., Cranor and Garfinkel 2005; Smetters and Grinter 2002). Thus, from a supplier perspective, it is important to understand customers' evaluation of both the functional and the dysfunctional characteristics of IT security safeguards in order to uncover customers' IT security risk protection requirements and to derive strategies that ensure effective and economical IT security safeguard development.

### 5.2.2 Hypothesis Development

In recent years, customer organizations have increasingly realized the important role of IT security in their systems. The demand as well as the market for IT security mechanisms is constantly growing (pwc 2015). Accordingly, several studies in IS research analyze IT security safeguards from an economic point of view (with optimization models of IT security investments) (e.g., Cavusoglu et al. 2008; Sonnenreich et al. 2006). IT security is an important issue for customer organizations, and based on their evaluation of an IT security safeguard, they are generally willing to make considerable investments for its implementation. Moreover, because the evaluation of IT security safeguards is determined by different customer requirements — the specific requirements individual customer organizations have for protection of an IT product against certain IT security risks — IT security risk protection requirements are strongly determined by their decision makers' perceptions of IT security risks. Thus, the implementation of IT security safeguards may have different impacts on satisfaction (Oliver 1980) and be associated with different levels of customer WTP (Sakao 2009). Hence, we hypothesize:

*H1: Different evaluations of IT security safeguards are associated with different levels of customer WTP.*

Based on the theoretical underpinnings of the Kano Theory, the five attribute categories in the context of IT security safeguards can be defined as follows:

Basic IT security safeguards are safeguards whose presence is a prerequisite for customer satisfaction. Their absence leads to dissatisfaction because the addressed IT security risks are perceived as relevant to the customer organization, and thus these safeguards represent the customer's minimal (basic) IT security risk protection requirements (Kano et al. 1984). However, a customer will not show an additional WTP for the implementation of these IT security safeguards, because their implementation is a precondition for considering adoption of an IT product (Matzler and Hinterhuber 1998; Sauerwein et al. 1996). Performance IT security safeguards lead to dissatisfaction if absent, but their implementation has a proportional effect on customer satisfaction. The addressed IT security risks are perceived as relevant, and thus IT security safeguards in this category meet the customer company's performance IT security risk protection requirements (i.e., a certain degree of implementation is needed to prevent dissatisfaction) (Kano et al. 1984; Matzler and Hinterhuber 1998; Sauerwein et al. 1996). Hence, customers will be more likely to show an additional WTP for the implementation of these safeguards. The implementation of advanced IT security safeguards has a disproportionate influence on satisfaction, but their absence does not lead to dissatisfaction (Kano et al. 1984). IT security safeguards in the advanced category address IT security risks of which customers are not aware. Nevertheless, these safeguards are evaluated as functional by customers. Thus, customers may show an additional WTP if the supplier implements these safeguards. Customers do not care about the presence or absence of indifferent IT security safeguards. Neither their implementation nor their absence influences satisfaction (Clegg et al. 2010; Matzler and Hinterhuber 1998; Nilsson-Witell and Fundin 2005; Sauerwein et al. 1996). The IT security risks addressed by this category of safeguards are not perceived as relevant by the customer. Additionally, dysfunctional characteristics of these IT security safeguards may not be perceived as critical. Since these IT security safeguards do not meet any IT security risk protection requirements, the customer will not be interested in making additional investments for them, i.e., will not show any additional WTP (Matzler and Hinterhuber 1998; Sauerwein et al. 1996). Reverse IT security safeguards are those that customers do not want to have implemented in their IT system, because they perceive these safeguards to be more dysfunctional than functional. The addressed IT security risks are not perceived as relevant, while the implementation is associated with dysfunctional characteristics, perhaps due to perceived restrictions or conflicting objectives. Consequently, the implementation of these safeguards will result in customer dissatisfaction (Nilsson-Witell and Fundin 2005). Accordingly, these safeguards will negatively influence customer WTP for

the IT product, especially if the market offers suitable alternatives. Table 13 provides an overview of the characteristics of the five IT security safeguard categories.

**Table 13: Characteristics of the IT Security Safeguard Categories**

Charac- teristics	IT Security Safeguard Categories				
	Basic	Performance	Advanced	Indifferent	Reverse
<b>Customers' IT Security Risk Protection Requirements</b>	The addressed IT security risks are perceived as relevant by the customer and implementation represents the minimal IT security risk protection requirements.	The addressed IT security risks are perceived as relevant and implementation meets the customers' IT security risk protection requirements.	The customer is not aware of the addressed IT security risks but perceives the implementation as functional.	The customer neither perceives the addressed IT security risks as relevant nor perceives the implementation as dysfunctional.	The customer does not perceive the addressed IT security risks as relevant but perceives the implementation as dysfunctional.
<b>Customer Satisfaction with IT Security Safeguard</b>	Non-implementation leads to dissatisfaction but implementation does not generate satisfaction.	Implementation leads to proportional satisfaction and non-implementation leads to proportional dissatisfaction.	Implementation disproportionately influences satisfaction but non-implementation does not generate dissatisfaction.	(Non-) Implementation produces neither satisfaction nor dissatisfaction.	Implementation leads to dissatisfaction.

Based on the influence of the different IT security safeguard categories on customer satisfaction and dissatisfaction, as described above, only the implementation of IT security safeguards evaluated as advanced or performance can generate customer satisfaction. Since advanced IT security safeguards potentially have the strongest influence on satisfaction, we hypothesize:

*H2: IT security safeguards evaluated as advanced are associated with a higher level of customer WTP than IT security safeguards that are evaluated as performance.*

The implementation of basic and indifferent IT security safeguards will not be associated with additional customer WTP because their implementation cannot generate customer satisfaction. As pointed out above, basic IT security safeguards can be seen as prerequisites for customers to consider the purchase of the supplier's IT product. In the case of indifferent IT security safeguards, the customer does not care about their implementation. Compared to basic and indifferent IT security safeguards, customers will show an additional WTP for the implementation of performance IT security safeguards because these positively influence customer satisfaction. In contrast, the implementation of reverse IT security safeguards in an IT product will lead to customer dissatisfaction and thus will be associated with less WTP. Based on these theoretical underpinnings, we hypothesize:

*H3: IT security safeguards evaluated as performance are associated with a higher level of customer WTP than IT security safeguards that are evaluated as basic, indifferent, or reverse.*

*H4: IT security safeguards evaluated as basic, indifferent, and reverse are not associated with a higher level of customer WTP.*

### **5.3 Research Methodology and Data Analysis**

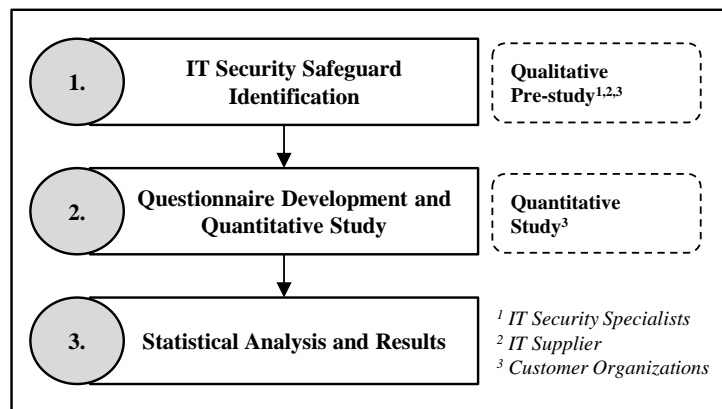
First, we conducted a qualitative pre-study in order to identify relevant and appropriate IT security safeguards before developing the questionnaire for the quantitative study. The research approach is shown in Figure 9 and is presented in detail in the following sections.

#### *5.3.1 IT Security Safeguard Identification*

For the pre-study, discussions were conducted between IT security security specialists and representatives of a leading enterprise software supplier. These began with a discussion of the definitions of the five IT security safeguard categories. Since including too many IT security safeguards in the quantitative study would negatively influence the response rate, four criteria were deemed relevant for the IT security safeguard selection process. First, the IT security safeguards (potentially) had to be relevant to a wide variety of customer organizations. Second, at least one IT security safeguard that is perceived as basic by most customers had to be represented. Third, IT security safeguards that are often brought up by customer organizations in negotiations with suppliers should be included to gather data covering different customer evaluations. Fourth, it was necessary that the principles underlying the selected safeguards should be understood by most of the surveyed customers. As a result, six

IT security safeguards were identified. Next, we prevalidated our measurement model and discussed the developed survey with two IT practitioners and three IS researchers. Based on the results of this phase, we conducted four qualitative interviews to obtain a deeper understanding of IT security safeguard evaluation as well as to verify our measurement model. We interviewed a CIO of a large organization in the mechanical engineering sector (#1), a CEO from a small organization in the real estate industry (#2), the CTO of a medium-sized e-commerce organization (#3), and an IT security specialist for a large transportation organization (#4). Thus, we obtained insights from different hierarchical positions and organizations. The average interview lasted 36 minutes, and the interviews were fully transcribed and coded.

As a result of this pre-study, the quantitative study is focused on the following six IT security safeguards: automatic installation of IT security updates, IT security certification of the supplier, multifactor authentication, full data encryption, role-based access control, and daily backups.



**Figure 9: Research Approach (Research Paper C)**

### 5.3.2 Questionnaire Development and Quantitative Study

Our quantitative study was conducted between October 30 and November 19, 2014. We contacted 61 decision makers from different organizations via an online social business network and a further 390 directly via e-mail. To encourage participation, a management report was offered to the participants. After two weeks of data collection, we reminded the contacts about the study via e-mail or messages in the business network. With 84 completed surveys, the response rate was 18.6%. Of the participants, 66.7% were CIOs, 11.9% IT security managers, 3.6% CEOs, 3.6% business managers, and 14.3% other managers. More than half (65.5%) of the companies were corporations (>249 employees), 28.6% were medium-sized companies (50–249 employees), and 6.0% were small companies (<50



employees). Among the participants, 81% had more than 11 years' professional experience, 14.3% 6–10 years, and 4.8% 1–5 years. Two main reasons were given for not participating: their organizations did not participate in such studies in general or there were time pressures.

Content validity was established by adopting validated measurement items from previous studies with minor changes in wording. For each of the six IT security safeguards, two questions (functional and dysfunctional) were formulated: “How do you evaluate the implementation [of the IT security safeguard, as specified above]?” and “How do you evaluate the non-implementation [of the IT security safeguard, as specified above]?” In accordance with previous research, five answers were possible: desirable, indispensable, neutral, acceptable, and negative. This construction and interpretation of the questionnaire has been widely used (e.g., Berger et al. 1993; Kano et al. 1984; Tan and Shen 2000). We also asked the participants to evaluate the degree of their WTP for each of the IT security safeguards: “For implementing [the IT security safeguard] our organization is willing to make...”, 1=no investments to 7=very high investments) (Liang and Xue 2010).

Since the 84 records could have differently distributed data about the six IT security safeguards, we standardized the stated WTP data to achieve comparability. After transforming the safeguard-specific variables into standardized scores, we had (comparable) data for each of the six IT security safeguards in every one of the 84 records (504 in total).

### 5.3.3 *Statistical Analysis and Results*

#### 5.3.3.1 *Different Evaluations of IT Security Safeguards*

Each IT security safeguard can be classified into one of the five categories of Kano's Theory of Attractive Quality by combining its functional and dysfunctional assessments (see Table 14) (Berger et al. 1993; Matzler et al. 2004b). Table 15 shows the outcomes of the categorization for the six IT security safeguards. The most common customer evaluations are highlighted in grey. The results indicate that daily backups are unambiguously assigned to the basic category (83.3% agreement). This finding is also validated by the results of the customer interviews conducted in the pre-study. All participants assessed daily backups as a common, standard practice. Customers evaluated the functional and dysfunctional characteristics differently for the other five IT security safeguards. Automatic updates and role-based access control were assessed to be basic by most of the participants, but more than 20% assessed these as performance IT security safeguards. The customer interviews indicated that automatic updates are sometimes perceived as dysfunctional because “this may fix

vulnerability but can also be associated with new risks” (#3) and “because of our complex IT systems, including legacy systems, we are often confronted with the conflict of securing the system and minimizing the operational impairment” (#4). In contrast, role-based access control was evaluated as basic — “lived praxis” (#1), “standard” (#2), “should be granted even in case of medium protection needs” (#4) — by all interviewees, because “access should be minimized to the necessary information” (#3).

### Table 14: IT Security Safeguard Evaluation Table

IT Security Safeguards		Dysfunctional				
		Desirable	Indispensable	Neutral	Acceptable	Negative
Functional	Desirable	Q	A	A	A	P
	Indispensable	R	I	I	I	B
	Neutral	R	I	I	I	B
	Acceptable	R	I	I	I	B
	Negative	R	R	R	R	Q
B: Basic, P: Performance, A: Advanced, I: Indifferent; R: Reverse, Q: Questionable						

**Table 15: Results of the IT Security Safeguard Categorization**

IT Security Safeguards	B	P	A	I	R	Q	Total	IT Security Safeguard Category
<i>n</i>	160	66	94	161	21	2	504	
Updates	34	17	11	14	8	0	84	Basic [Performance]
Certification	2	7	31	44	0	0	84	Indifferent [Advanced]
Multifactor Authentication	8	10	21	40	4	1	84	Indifferent [Advanced]
Data Encryption	6	7	21	43	7	0	84	Indifferent [Advanced]
Role-based Access Control	40	19	8	14	2	1	84	Basic [Performance]
Backups	70	6	2	6	0	0	84	Basic
B: Basic, P: Performance, A: Advanced, I: Indifferent, R: Reverse, Q: Questionable								

With regard to IT security certification of the supplier, multifactor authentication, and full data encryption, most of the participants in the quantitative study were indifferent, although more than 24% assigned these safeguards to the advanced category. Our qualitative results indicate doubt about the effectiveness of certifications: “This is a nice to have [...] but may be associated with more efforts than benefits” (#1), a “kind of false sense of security [...] with regard to the actual cost–benefit analysis” (#2), “The risk can be reduced [...] but is also a matter of interpretation” (#4), “certification [might be] necessary due to [environmental] requirements” (#3). Opinions about multifactor authentication differed: “My colleagues would not be amused” (#1), “this would be very useful” (#2, #3), “but implementation is difficult, because of restrictions on usability; on some days, I am performing dozens of logins” (#3). Thus, it can be concluded that multifactor authentication is fundamentally associated with perceived risk reduction but the effort is perceived as outweighing the benefits. One comment about full data encryption was: “We do not see the necessity of full data encryption because it is associated with effort but no benefits for us. But if it would be implemented it would not bother me” (#1). Another was that full data encryption might result in availability problems (#3). In summary, the quantitative results indicate that basic IT security safeguards are often also perceived as performance IT security safeguards, and indifferent IT security safeguards as advanced ones. Our qualitative data show that these different evaluations are caused by different IT security risk protection requirements.

In previous studies, questionable results (which are shown in Table 14) were typically deleted for the quantitative analysis (e.g., (Berger et al. 1993; Sauerwein et al. 1996)). Thus, we removed the questionable IT security safeguard evaluations and performed the following quantitative analysis with a sample size of 502. Because our data show only two questionable results (Table 15), this indicates that our functional and dysfunctional questions did not suffer from phrasing problems (Kano et al. 1984).

### 5.3.3.2 WTP associated with Different IT Security Safeguard Categories

The Shapiro-Wilk-Test indicated that our quantitative data are not normally distributed. Accordingly, we tested our hypotheses by using nonparametric statistics. In a first step, we applied the Kruskal-Wallis-Test to examine whether the five Kano categories are generally associated with different levels of customer WTP. The results show that significant differences between the five IT security safeguard categories exist (chi-square 20.283; df 4; asymp. sig. 0.000), supporting H1. Moreover, we introduced two group variables as shown in Table 16. To investigate between which groups and categories significant differences in

customer WTP exist, we used the Mann-Whitney-U-Test. The results of the analyses are shown in Tables 16 and 17. Significant differences are highlighted in grey. The average values of customers' WTP within the different categories are shown in Table 18.

**Table 16: Results for the Group Variables**

<b>Group Variable</b>	<b>Group 1</b>	<b>Group 2</b>	<b>Sig.</b>
<b>d1</b>	A	P, B, I, R	0.014
<b>d2</b>	P	B, I, R	0.000
B: Basic, P: Performance, A: Advanced, I: Indifferent, R: Reverse			

**Table 17: Results for Different Levels of WTP within the IT Security Safeguard Categories**

<b>Significant Differences for WTP</b>	<b>P</b>	<b>B</b>	<b>I</b>	<b>R</b>
<b>A</b>	0.351	0.416	0.000	0.001
<b>P</b>		0.127	0.000	0.001
<b>B</b>			0.000	0.011
<b>I</b>				0.229
B: Basic, P: Performance, A: Advanced, I: Indifferent, R: Reverse				

**Table 18: Descriptives for Customers' WTP**

<b>IT Security Safeguard Category</b>	<b>n</b>	<b>Mean</b>	<b>Std. Dev.</b>
<i>Group 1 (d1)</i>	408	-0.054	0.994
<i>Group 2 (d2)</i>	342	-0.135	0.974
<i>Basic</i>	160	0.092	1.051
<i>Performance</i>	66	0.366	0.998
<i>Advanced</i>	94	0.236	0.975
<i>Indifferent</i>	161	-0.311	0.857
<i>Reverse</i>	21	-0.517	0.835

Regarding the differences between customers' WTP for advanced IT security safeguards and for the other IT security safeguard categories, the Mann-Whitney-U-Tests showed significant results for the comparison of the advanced and indifferent IT security safeguard categories as

well as for the comparison of the advanced and reverse categories. The average customer WTP for indifferent (-0.311) and reverse (-0.517) IT security safeguards were significantly lower than the WTP for advanced IT security safeguards (0.236; see Table 18). Nevertheless, no significant differences between performance and advanced IT security safeguards were found. Moreover, the average WTP for advanced IT security safeguards (0.236) was lower than the WTP for performance IT security safeguards (0.366; see Table 18). Thus, H2 has to be rejected. However, the Mann-Whitney-U-Test revealed significant differences between IT security safeguards evaluated as advanced and those evaluated as performance, basic, indifferent, or reverse (Table 16). As shown in Table 18, the average WTP for advanced IT security safeguards was 0.236 and thus higher than the mean for the IT security safeguards perceived as performance, basic, indifferent, or reverse (-0.054).

Furthermore, the Mann-Whitney-U-Test showed that customers' WTP for performance IT security safeguards was significantly different from their WTP for IT security safeguards that have less or no influence on customer satisfaction (i.e., basic, indifferent, and reverse safeguards; see also Table 16). The average customer WTP for performance IT security safeguards was 0.366, and for the other three categories it was -0.135 (see Table 18). Consequently, H3 is supported. In particular, the WTP for performance IT security safeguards was significantly different compared to IT security safeguards evaluated as indifferent and reverse. The means for indifferent (-0.311) and reverse IT security safeguards (-0.517) were lower than the mean for performance IT security safeguards (see Table 18). However, no significant differences between performance and basic IT security safeguards were found (see Table 17). Thus, the results show that the customers' WTP for IT security safeguards evaluated as performance was significantly higher than their WTP for IT security safeguards evaluated as indifferent or reverse. Moreover, the comparisons between basic and indifferent and between basic and reverse IT security safeguards yielded significant differences in customers' WTP (see Table 17). Indifferent IT security safeguards had a mean WTP of -0.311 and reverse IT security safeguards a mean of -0.517 (see Table 18), while the average WTP for basic IT security safeguards (0.092) was significantly higher. The results in Table 18 indicate that the customers did not show additional WTP for the implementation of IT security safeguards that they perceive as basic. The standardized mean value of customers' WTP for basic IT security safeguards is close to zero. Moreover, IT security safeguards that were evaluated as indifferent or reverse by the customers tended to be associated with a lower level of WTP. However, the average customer WTP for basic IT security safeguards was found to be significantly higher than their WTP for indifferent or reverse IT security

safeguards. Nonetheless, the mean values for customers' WTP indicate that H4 can be regarded as supported.

Overall, our results show that while there are no significant differences between customers' WTP for basic, performance, and advanced IT security safeguards, there are significant differences between their WTP for these three categories and their WTP for indifferent and reverse IT security safeguards. While the additional WTP for IT security safeguards that are perceived as basic was close to average, the WTP for IT security safeguards evaluated as performance and advanced was well above average. Accordingly, these IT security safeguards are associated with a higher customer WTP.

### 5.3.3.3 Impact on Satisfaction and Dissatisfaction

The Kano Theory also allows conclusions to be drawn regarding the effects of the implementation or non-implementation of certain IT security safeguards on customer satisfaction. We determined the customer satisfaction (CS) and customer dissatisfaction (CD) coefficient as suggested by previous research (e.g., Berger et al. 1993; Clegg et al. 2010; Matzler and Hinterhuber 1998; Sauerwein et al. 1996). For calculating the average impact on satisfaction (CS), advanced (A) and performance (P) IT security safeguards are of interest because these IT security safeguards have the potential to produce customer satisfaction if implemented by the supplier. Similarly, for determining the average impact on customer dissatisfaction (CD), basic (B) and performance IT security safeguards are of interest as these IT security safeguards will cause customer dissatisfaction if they are not implemented in the supplier's IT products. The implementation of IT security safeguards that customers are indifferent (I) about produce neither satisfaction nor dissatisfaction. The formulas are as follows:

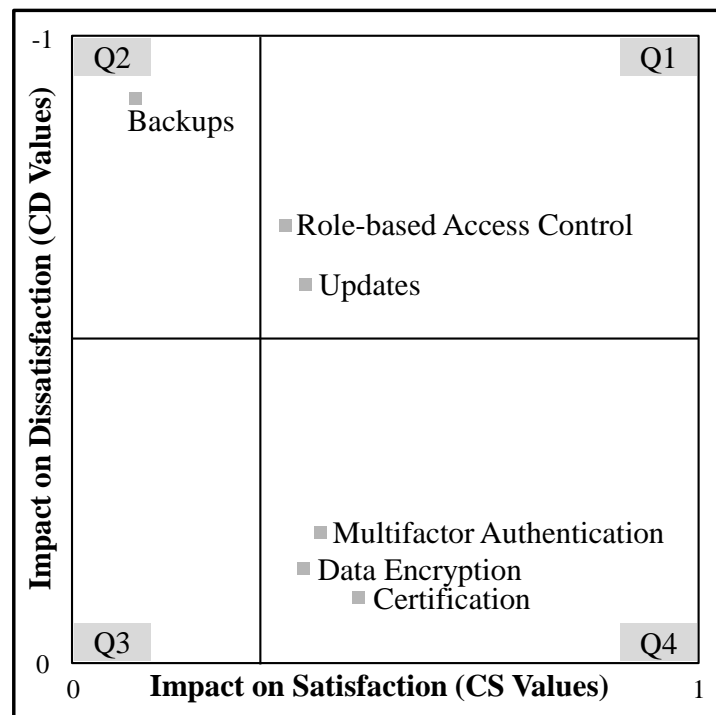
$$CS = \frac{A + P}{A + P + B + I} \quad CD = - \frac{P + B}{A + P + B + I}$$

The values of CS and CD for each of the six IT security safeguards are presented in Table 19. A graphical overview of potential influences on customer satisfaction and dissatisfaction is provided in Figure 10. The x-axis represents the impact on satisfaction (CS values) and the y-axis the impact on dissatisfaction (CD values). The partition lines represent the means of the satisfaction and dissatisfaction coefficients. Accordingly, the higher an IT security safeguard is positioned above the horizontal line, the greater the dissatisfaction that is produced when the IT security safeguard is not implemented by the supplier (Q1 and Q2). The further an IT

security safeguard is positioned to the right of the vertical line (Q1 and Q4), the greater the satisfaction that is associated with its implementation in the IT product. Consequently, IT security safeguards positioned in Q1 produce more satisfaction than IT security safeguards in Q2. The influence of IT security safeguards in Q3 on both customer satisfaction and dissatisfaction is below average. However, IT security safeguards in Q4 have above-average potential to cause satisfaction. From the suppliers' perspective, the resulting four areas can be useful for deriving appropriate strategies.

**Table 19: Impact on Customer Satisfaction**

IT Security Safeguards	CS Values	CD Values
<i>Updates</i>	0.368	-0.607
<i>Certification</i>	0.452	-0.107
<i>Multifactor Authentication</i>	0.392	-0.214
<i>Data Encryption</i>	0.364	-0.155
<i>Role-based Access Control</i>	0.333	-0.702
<i>Backups</i>	0.095	-0.905
CS: Customer Satisfaction, CD: Customer Dissatisfaction		



**Figure 10: Impact on Satisfaction and Dissatisfaction**

## 5.4 Discussion

The aim of this study was not only to advance our understanding of how IT security safeguards implemented in IT products are evaluated by customer organizations but also to expand our knowledge of the impact of different IT security safeguard evaluations on customers' associated WTP. Understanding this trade-off for risks vs. costs on the customer side will enable IT suppliers to optimize their decision making about investments in developing and implementing different safeguards in their products.

Based on a large-scale empirical study and qualitative interviews, we were able to demonstrate that the appropriateness of an IT security safeguard that is implemented in an IT system may be perceived differently by different customer organizations. In particular, the very same IT security safeguard might be a basic requirement for one customer company but assessed as counterproductive by another. We show that these heterogeneous evaluations are generally associated with different levels of customer WTP. Customers are willing to invest more money when they perceive an IT security safeguard as more functional than dysfunctional (i.e., advanced, performance, or basic). In contrast, when an IT security safeguard is perceived as indifferent or as more dysfunctional than functional (i.e., reverse), customers show a significantly lower level of WTP for its implementation. Contrary to our expectations, we did not find significant differences between customers' WTP for advanced, performance, and basic IT security safeguards. One reason for this finding might be that customers tend to evaluate an IT security safeguard as basic when the organization is aware of the safeguard and the IT security risks it addresses. If customers have insufficient information about the IT security safeguard, they might tend to be indifferent (e.g., they might not perceive the addressed IT security risk to be relevant). Future research could enrich this study's findings by gathering a larger number of different customer evaluations of IT security safeguards and controlling for awareness of the functional and dysfunctional characteristics of the analyzed safeguards. This might offer more detailed information about the differences between basic, performance, and advanced IT security safeguards as well as their differences from IT security safeguards that are perceived as indifferent and reverse.

This study makes several contributions to IS research and practice. To the best of our knowledge, we are the first to adapt Kano's Theory to the IT security context. Our study highlights the importance of considering the assessment of both the functional and the dysfunctional characteristics of safeguards; these are often neglected by IT security studies, especially in the organizational context (e.g., Cavusoglu et al. 2015). Future research can



build on our results when analyzing evaluations of safeguarding measures in different fields of application. For example, the results of this study are important for mathematical optimization models. Furthermore, our study will enable researchers to better understand and predict the outcome of IT security management decisions by considering the multidimensional nature of IT security safeguard evaluation in terms of the five IT security safeguard categories. Understanding the multidimensional nature of IT security safeguard evaluation might also allow future research to reinvestigate behavioral phenomena in the IT security context that are yet unclear (e.g., why people decide not to adopt safeguarding measures even when they perceive the addressed risks to be very critical (e.g., Johnston and Warkentin 2010)). As our proposed framework can be applied to investigate how a product's IT security is assessed by customer companies, managers of IT suppliers can particularly benefit from this study. Based on the developed set of questions presented in the data analysis part of this study, IT suppliers can analyze how the safeguards implemented in their products influence their customers' satisfaction and hence their associated WTP. Following this study's approach, they can effectively identify which safeguards should be implemented, improved, or removed from the product. For example, the customer satisfaction and dissatisfaction (CS and CD) values for Q2 in our study show that non-implementation of a basic IT security safeguard (daily backups in our example) largely creates customer dissatisfaction. Suppliers should therefore definitely implement these IT security safeguards in their product (Sakao 2009); otherwise, their product may not be competitive. The two IT security safeguards in Q1 (automatic updates and role-based access control in our example) also cause dissatisfaction when they are not implemented but have a greater impact on satisfaction when they are implemented. IT security safeguards that are mainly evaluated as performance should be further enhanced by the supplier, depending on the costs and customers' WTP (Sakao 2009). The influences of the IT security safeguards in Q3 on customer satisfaction and dissatisfaction are both below average. Thus, removal of the IT security safeguards in Q3 has the potential to considerably reduce costs for suppliers since customers seem to be mostly indifferent about their implementation (Sakao 2009). The IT security safeguards in Q4 (multifactor authentication, full data encryption, and certification in our example) have above-average potential to result in satisfaction. From the suppliers' perspective, these safeguards therefore have the potential to produce a competitive advantage. If IT security safeguards are perceived mainly as indifferent or advanced (see Table 15), suppliers should reconsider their implementation. The implementation of advanced IT security safeguards may bring a competitive advantage, but investing in the development of (future) indifferent IT security

safeguards will most likely result in financial losses. In this regard, due to the dynamic nature of product attributes (Nilsson-Witell and Fundin 2005), IT security safeguards might be evaluated as indifferent because customers are not aware of the addressed IT security risks and therefore do not have the corresponding IT security risk protection requirements. However, their perception of the addressed IT security risks might change over time based on new information or other environmental factors. That is, the evaluation of an IT security safeguard can shift from indifferent to advanced and thus represent a future competitive advantage for suppliers (Nilsson-Witell and Fundin 2005). Nevertheless, if an IT security safeguard is not promising from either the supplier's or the customer's perspective, the supplier should not further invest in its development and implementation. Reverse IT security safeguards should generally be removed, because their implementation only produces customer dissatisfaction and might therefore represent a competitive disadvantage.

### **5.5 Limitations, Future Research, and Conclusion**

Three limitations of this study merit consideration. First, we analyzed a subset of IT product safeguards. Future research can enrich our study's results by empirically investigating the evaluation of a larger number of safeguarding measures. Second, our study focuses on the top echelon's assessment of IT security safeguards. Even if these decision makers are ultimately responsible for the organizations' IT and trigger the final decisions, other managers and employees might be involved as well and thus influence organizational IT decisions. Hence, we encourage future research to investigate the IT management process in depth at different hierarchical levels of organizations. Third, our study is cross-sectional and static. We did not study the decision makers' IT security safeguard evaluations longitudinally and thus did not consider the influence of time on the perception of IT security safeguards. It is conceivable that an IT security safeguard might be viewed as indifferent or advanced at the outset but then, after a certain period of time, come to be perceived as performance or basic, e.g., because the organization has become aware of the addressed IT security risk or the perceived effort changes (Nilsson-Witell and Fundin 2005). Future research should explore this dynamic as well. These studies might also examine the effects of potential errors in the decision makers' assessments of IT security risks and the prioritization of IT security risk protection requirements (e.g., Loske et al. 2013) in order to perform an appropriate importance–performance analysis (Matzler et al. 2004a). Moreover, potential antecedents of IT security safeguard evaluations should also be included in these studies. IT security risk protection

requirements might be influenced not only by the perceived IT security risks but also by other factors (e.g., legal requirements or other stakeholders).

Overall, our study advances the understanding of customers' evaluations of IT security safeguards and has several theoretical and practical implications. The results highlight that IT suppliers should carefully consider customers' IT security needs when making decisions about the IT security in their IT products. By doing so, suppliers can derive effective strategies to gain economic and competitive advantages.

## 6 Research Paper D: Managers' Status Quo-Thinking

**Title:** Never Change A Running System? How Status Quo-Thinking Can Inhibit Software As A Service Adoption In Organizations

**Authors:** Heidt, Margareta  
Sonnenschein, Rabea  
Loske, André

**Published in:** Proceedings of the 25<sup>th</sup> European Conference on Information Systems (ECIS), Guimarães, Portugal 2017

### Abstract

*Despite the “buzz” about Software as a Service (SaaS), decision makers still often refrain from replacing their existing in-house technologies with innovative IT services. Industry reports indicate that the skeptical attitude of decision makers stems primarily from a high degree of uncertainty that exists, for example, due to insufficient experience with the new technology, a lack of best practice approaches, and missing lighthouse projects. Whereas previous research is predominantly focused on the advantages of SaaS, behavioral economics conclusively demonstrate that reference points like the evaluation of the incumbent technology or a familiar product are oftentimes prevalent when decisions are made under uncertainty. In this context, Status Quo-Thinking may inhibit decisions in favor of potentially advantageous IT service innovations. Drawing on Prospect Theory and Status Quo Bias research, we derive and empirically test a research model that explicates the influence of the incumbent technology on the evaluation of SaaS. Based on a large-scale empirical study, we demonstrate that the decision makers' attitude toward SaaS is highly dependent on their current systems and their level of SaaS. A lack of SaaS experience will increase the impact of the Status Quo, thus inhibiting a potential advantageous adoption of the new technology.*

**Keywords:** Status Quo Bias, Prospect Theory, Software as a Service (SaaS), Adoption.

## 6.1 Introduction

The World Economic Forum stated already in 2010 that “in addition to reducing operational costs, cloud technologies have become the basis for radical business innovation and new business models, and for significant improvements in the effectiveness of anyone using information technology” (World Economic Forum 2010, p. 1). Fittingly, recent analyses of research institutes forecast the public cloud services market to reach a total of \$204 billion in 2016 (e.g., Gartner 2016; IDC 2016; Synergy 2016). A substantial part of that growth is contributed to Software as a Service (SaaS) — the provisioning of applications running on a cloud infrastructure — that will remain the dominant public cloud computing type at an estimated 20.3 percent growth rate resulting in forecasted revenues of roughly \$37.7 billion in 2016 (e.g., Cisco 2016; Gartner 2016; IDC 2016). Associated with a large variety of benefits like scalability, mobility or cost savings that are increasingly affirmed by practitioners, SaaS has been hailed as the future default software delivery solution (e.g., Dahlberg et al. 2017). Unsurprisingly, IDC predicts that the penetration of SaaS solutions compared to traditional software deployment will be over 25 percent by 2020 (IDC 2014b). However, especially current European reports show that nearly 80 percent of EU enterprises still do not use cloud services implying that adoption rates are not as high as expected (Eurostat 2016). Given its role as state-of-the-art technology and innovative service model in an evolving business environment, it is thus crucial to understand why many decision makers today still refrain from using SaaS in a business environment shaped by increased mobility and disruptive marketing strategies (e.g., Lin and Chen 2012).

Previous research explains the non-adoption of SaaS in organizations either with legal or strategic requirements to keep data processing completely in-house or as the result of a risk-benefit-analysis (e.g., Benlian and Hess 2011). Whereas theoretical studies mostly consider purely rational decision makers, experts claim that decision makers “have been more protective of their existing infrastructure and, in many cases, have been the biggest obstacle to cloud-based solutions” (van der Meulen and Rivera 2015). This non-rational behavior is a common assumption in behavioral economics studies when analyzing decisions that are made under uncertainty. Decision makers actually violate the axioms of rational choice under uncertainty due to cognitive biases or “shortcuts” that compensate for a lack of information or experience (Tversky and Kahneman 1975). To account for these shortcuts, Kahneman and Tversky (1979) established the so-called Prospect Theory. This theory postulates that people faced with a decision under uncertainty will derive utility from gains and losses measured in relation to some reference points rather than on final assets. The dependence on reference

points has been frequently discussed in individual strategic choice contexts and was demonstrated in several empirical studies on the assessment of new products and services (e.g., Bamberger and Fiegenbaum 1996; Shoham and Fiegenbaum 2002). Surprisingly, the SaaS technology adoption literature has largely overlooked this reference-dependence although the decision to adopt SaaS generally entails a high degree of uncertainty due to the unknown complexity of IT security risks, lack of previous experience with cloud-based technologies, or missing best practices and lighthouse projects in the industry (e.g., Eduserv 2015; Eurostat 2014; Lin and Chen 2012). The decision to be protective of their existing (incumbent) infrastructure, i.e., the exaggerated preference for maintaining the current state of affairs, hints at another cognitive bias, namely the influence of Status Quo-Thinking (Samuelson and Zeckhauser 1988). Status Quo Bias itself has been demonstrated in a wide range of studies of consumer and investment behavior and is increasingly used in management of information systems (MIS) research (Fleischmann et al. 2014). However, research on software selection and particularly studies investigating the intention to adopt cloud based services did not account for this cognitive bias in decision making.

To account for this research gap, we first investigated the influence of reference-dependence on SaaS adoption at the organizational level and from there, analyzed how this dependency is affected by Status Quo-Thinking (e.g., Gerlach et al. 2014; Schweitzer 1995). The distinctiveness of the Status Quo Bias depends on the degree of uncertainty, i.e., the lack of information and experience decision makers are faced with. Based on the data of a large scale empirical study with decision makers in charge of the organizational IT, we confirmed our assumptions in a two-step approach: In the first step, we demonstrate the strong influence of the assessment and prevalence of the incumbent in-house technology on decision makers' attitudes toward a new technology — in our case SaaS. In our second step, we uncover the effect of the Status Quo Bias by comparing experienced and non-experienced or less-experienced decision makers. We specifically chose SaaS as a clearly definable object of investigation given that the majority of organizations will need to evaluate whether to adopt SaaS as a new technological service model now or in the near future due to the increasing amount of data processing and the demand for mobility (e.g., McLellan 2016; Rivera and van der Meulen 2014).

Our study provides several theoretical and practical implications. Given that virtually all technology adoptions nowadays imply a replacement decision, our study highlights the relevance of reference-dependence in MIS research. In this regard, it is essential for future IS

research to acknowledge that Status Quo-Thinking has a profound effect on decision-making processes regarding new technology acceptance in organizations. Our findings are also highly relevant to both providers of SaaS and decision makers of (potential) customer organizations. Providers should consider the varying degrees of Status Quo-Thinking and group their customers according to their level of SaaS experience. These identified customer groups can be addressed appropriately and more effectively by adapting marketing and sales strategies accordingly, whereas decision makers need to acknowledge the role of reference points and Status Quo-Thinking to avoid missing out on beneficial technological developments. Joining expert roundtables or including objective assessors could reduce the influence of the Status Quo Bias in decision-making processes. These measures can reduce the possibility that Status Quo-Thinking inhibits SaaS adoption even if the new technology would objectively be the better option.

## **6.2 Theoretical Background and Hypothesis Development**

### *6.2.1 Technology Adoption Models and Rational Choice*

There is a rich tradition in technology acceptance and adoption research. The theories primarily used to study the acceptance and adoption of innovations in information systems or information technologies generally originate in social psychology, such as Theory of Reasoned Action (TRA) (Ajzen and Fishbein 1980) and its extension Theory of Planned Behavior (TPB) (Ajzen 1985). Drawing on TRA, many researchers added constructs or derived new models such as Davis (1986) Technology Acceptance Model (TAM) or Venkatesh et al. (2003) who later consolidated the aforementioned and five further models into the Unified Theory of Acceptance and Use of Technology (UTAUT).

Despite different factors and research model designs, the majority of studies base their assumptions on rational choice, i.e., the rational weighing up of costs and benefits concerning the technology adoption. Specifically, perceived risks and perceived benefits are often singled out and commonly considered as decisive antecedents of behavioral intention or attitude toward SaaS (e.g., Benlian and Hess 2011) or sometimes described as drivers and inhibitors of SaaS adoption (e.g., Benlian et al. 2009; Lee et al. 2013). Several studies look at risks and benefits as relative advantage, i.e., already implicitly weighing up potential benefits of a new technology with the current advantages of the incumbent technology (e.g., Chau 1996; Wu and Wang 2005).

In line with the predominant literature stream, we draw on a benefit-risk framework in an organizational setting. Previous research oftentimes studied differences in the perceptions of IT executives' in both SaaS adopter and non-adopter firms, but they did not link the differences they found directly to cognitive biases (Benlian and Hess 2011). Contrarily, consumer studies went further and highlighted the importance of reference points as an "anchor" for decisions to either replace or stick to the incumbent technology or product (Moqbel and Bartelt 2015; Roster and Richins). This dependence on reference points often explains the influence of the incumbent technology when people have to analyze the relative advantage of a new technology during a decision-making process under uncertainty (e.g., Gerlach et al. 2014). Accordingly, it is important to consider Prospect Theory and Status Quo research in the context of organizational SaaS adoption.

### *6.2.2 Prospect Theory, Status Quo Bias, and Hypothesis Development*

Prospect Theory was designed to analyze decision-making processes under uncertainty by considering so-called certainty and isolation effects (Kahneman and Tversky 1979). These two effects assume that decisions do not necessarily follow mathematical optimality (i.e., the rational weighing up of risks and benefits and their probability weights) due to several reasons: people either underestimate hardly probable outcomes in comparison with certain outcomes and/or people base their decisions rather on change of wealth than on total wealth, i.e., an absolute outcome (Kahneman and Tversky 1979). Accordingly, Prospect Theory postulates that decision makers' value functions are rather dependent on reference points than on the actual final outcome. These reference points are defined as the neutral position used by decision makers in order to determine the extent to which the expected outcomes of a decision constitute gains (i.e., above this position) or losses (i.e., below this position) (Kahneman and Tversky 1979). Kahneman and Tversky (1984) argue that individuals set up mental accounts to specify advantages and disadvantages associated with the offered option(s) when faced with a transaction or trade decision relative to a certain reference point. Several studies used Prospect Theory to analyze strategic choice and risk/return tradeoffs in organizational decision making (e.g., Fiegenbaum et al. 1996; Shoham and Fiegenbaum 2002; Sinha 1994). It is argued, therefore, that managerial decision processes often depend on reference points because many decisions must be made without advanced knowledge of their full impact and are thereby made under uncertainty. A similar utilization of reference points is at times applied in replacement decisions regarding consumer goods (e.g., Gerlach et al. 2014; Roster and Richins 2009).



Based on the theoretical underpinnings of Prospect Theory, it can be assumed that a replacement decision in the context of technology adoption generally entails a decision between opting for a new technology or maintaining the incumbent technology, i.e., the enterprise software that is currently hosted and operated in-house on the organization's IT infrastructure. An aggravating factor is the lack of historical data and experiences that inhibits a well-informed, more rational decision-making process. The absence of information or experience is pervasive in the context of service innovations as lighthouse projects and hard facts about the realization of assumed risks and benefits are missing. To overcome this issue, it can be assumed that the incumbent technology will serve as a reference point for the assessment of a new technology (e.g., Kahneman and Tversky 1979; Shoham and Fiegenbaum 2002). Consequently, decision makers will compare the new technology with the incumbent technology because experience and knowledge are available due to the familiarity in this regard. For example, when it comes to the decision whether to replace an existing in-house application with a new SaaS application, we assume that the attitudinal beliefs toward incumbent in-house technologies (i.e., attitudinal beliefs toward the currently used, well-known technology) will serve as reference points for the decision makers when forming the attitudinal beliefs toward new, yet partly unknown, SaaS technologies. As our research model is based on a risk-benefit framework frequently utilized by previous research in technology adoption (e.g., Benlian and Hess 2011), the attitudinal beliefs are formed by the juxtaposition of perceived benefits and risks. Therefore, the decision makers perceived benefits of a new SaaS technology will be influenced by the perceived benefits of the incumbent in-house systems that serve as a reference point. Furthermore, decision makers with little knowledge and experience will tend to underestimate the perceived benefits of SaaS in comparison with their familiar incumbent system. If the level of perceived benefits of the incumbent system is high, replacing this system will be regarded as futile. Logically, decision makers who are fully satisfied with their current in-house system will not regard the potential benefits of a new SaaS solution as equally high. Simultaneously, a decision maker who perceives the in-house system, for example, as costly and unreliable, will be more prone to change and will not consider this deviation from a certain outcome (i.e., subsequent use of the incumbent system) as a loss. Accordingly, decision makers who perceive the risks of their incumbent system as high, are more likely to consider a new SaaS technology to be less risky. Therefore, we hypothesize:

*H1a: Perceived benefits of in-house systems are negatively associated with the decision makers' perceived benefits of SaaS.*

Analogously, we assume the same influence regarding the evaluation and reference-dependence of the perceived risks:

*H1b: Perceived risks of in-house systems are negatively associated with the decision makers' perceived risks of SaaS.*

The benefits and risks associated with a new technology are fundamental in technology adoption decisions. Thus, previous studies in SaaS adoption show that behavior and intentions are largely determined by weighing up risks and benefits (e.g., Benlian and Hess 2011). These overall perceived risks and benefits include financial, strategic, security, performance, and management dimensions (Benlian and Hess 2011). In line with previous SaaS research (e.g., Benlian and Hess 2010; Benlian and Hess 2011; Lee 2009), we expect perceived risks to generally have a negative impact on decision makers' intentions to adopt a SaaS technology. For example, if decision makers perceive a high risk of downtime errors and data loss to be associated with SaaS technologies, they will be less likely to consider an adoption of this new SaaS technology. On the other hand, the perceived benefits are generally expected to positively influence decision makers' intentions to adopt. For example, if decision makers perceive SaaS technologies to be associated with potential cost reductions (e.g., due to lower server administration costs) their intention to adopt SaaS will be positively influenced. Therefore, high perceived benefits will more likely lead to an intention to adopt, whereas the perceived risks of SaaS will inhibit the intention to adopt. Accordingly, we further hypothesize:

*H2a: Perceived benefits of SaaS are positively associated with the decision makers' intention to adopt SaaS.*

*H2b: Perceived risks of SaaS are negatively associated with the decision makers' intention to adopt SaaS.*

Building on Prospect Theory and several experiments, Tversky and Kahneman (1985) discovered that decision makers prefer to be passive and inactive rather than experiencing negative results due to their actions or decisions. Some literature refers to this concept as reference point bias (Levy 1997), whereas a more common stream of research coined the term Status Quo Bias as an effect of the loss aversion discussed in Prospect Theory (Kahneman et al. 1991; Samuelson and Zeckhauser 1988). Loss aversion entails an overestimation of certain positive outcomes, whereas potential losses are weighted disproportionately. This demonstrates the preference for the current state of affairs, i.e., if individuals take the Status Quo as a reference point, then they will perceive any deviation from it as loss. Therefore, a

decision maker will avoid change and an unknown outcome unless the advantages clearly outweigh the perceived disadvantages. Another explanation for the Status Quo Bias is provided by Zajonc (1968) and Bornstein (1989) who argue that mere exposure to a stimulus (i.e., the incumbent product) enhances the attitude toward it and, therefore, argue that familiarity leads to liking.

A well-known example for the maintenance of the Status Quo is the QWERTY keyboard. Although a different arrangement of letters could lead to a more productive and better keyboard, QWERTY is still omnipresent because switching from the Status Quo could entail huge costs of retraining individuals and replacing the current design in systems and devices (David 1985). Especially, research on replacement decisions regarding (technological) consumer goods consider these high potential switching costs to inhibit a change from the Status Quo (e.g., Moqbel and Bartelt 2015; Roster and Richins 2009). Studies focusing on technology systems are increasingly building on these findings adding further contributing factors like habit or inertia (Kim and Kankanhalli 2009; Polites and Karahanna 2012). Almost all of these studies attribute the Status Quo Bias at least partially to insufficient available information and experience. Past experiences serve as an “anchor” or “frame” for decisions as decision makers frequently do not exclusively follow rational concepts of mathematical optimality (e.g., Schwenk 1984; Slovic 1975).

In line with previous research, we expect that decision makers in companies that already possess a certain degree of knowledge and past experience will demonstrate a lower Status Quo Bias in comparison to less or non-experienced decision makers. Decision makers with a low level of SaaS experience, will be more affected by the Status Quo Bias because they overestimate the losses that they would encounter when replacing the incumbent technology. Therefore, the correlation postulated in hypotheses H1a and H1b will be increased. On the other hand, decision makers who already possess a SaaS solution among their incumbent in-house technology will draw on the experience that they already accumulated with SaaS. Therefore, their decision-making process will be better informed and consequently less affected by Status Quo-Thinking. Greater experience and further facts available to decision makers will enable a more “rational” decision making process (Bazerman and Moore 2008). For example, experienced decision makers can judge the perceived benefits like cost reductions without drawing upon a comparison to their incumbent system because a previous adoption of a SaaS technology already proved to be cost-efficient. Similarly, experienced decision makers will evaluate the perceived risks of SaaS depending on past experience and

be less affected by Status Quo Bias. Whereas, inexperienced decision makers might, for example, believe that downtime issues are more pronounced in contrast to their reliable in-house technology and will thus attribute higher perceived risks to a new SaaS technology. Hence, we hypothesize:

*H3a: Perceived benefits of in-house systems will have a stronger negative association with the perceived benefits of SaaS for organizations with no or low SaaS experience than for organizations with SaaS experience.*

*H3b: Perceived risks of in-house systems will have a stronger negative association with the perceived risks of SaaS for organizations with no or low SaaS experience than for organizations with SaaS experience.*

The research model is shown in Figure 11.

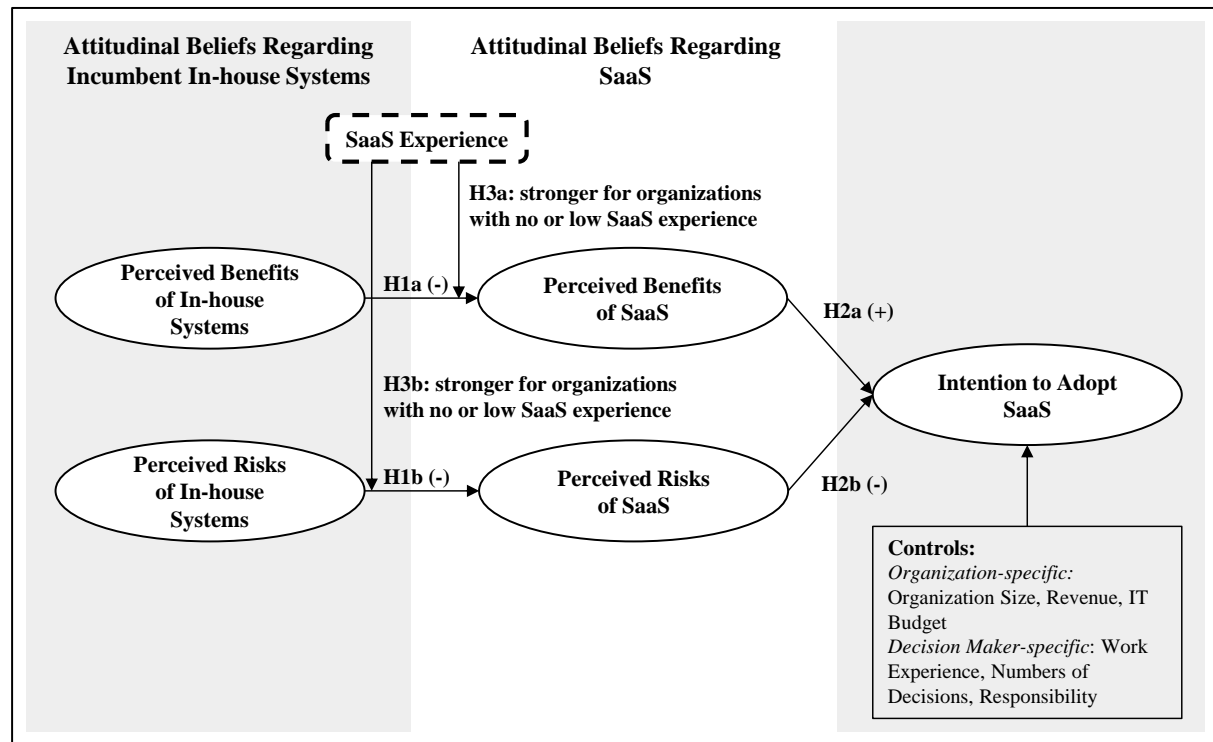


Figure 11: Research Model (Research Paper D)

## 6.3 Research Methodology and Data Analysis

### 6.3.1 Survey Administration and Sample Characteristics

Construct validity was established by adopting validated measurement items from previous research studies with minor changes in wording. All latent constructs were reflective and measured with multiple items on a 7-point Likert scale. To ensure a consistent understanding

of enterprise software in case of in-house systems and in case of SaaS, we used the following definitions within the study:

- **Enterprise software** is defined as business applications, such as Customer Relationship Management (CRM) systems, Enterprise Resource Planning (ERP) systems, or Project Management (PM) applications.
- **SaaS** is defined as enterprise software provided by a supplier and accessible via a public network, such as the Internet (i.e., public cloud).
- **In-house systems** are defined as enterprise software that is hosted and operated on the organization's IT infrastructure.

As suggested by previous research, we included work experience (in years), numbers of sourcing decisions already made, the responsibility for sourcing decisions in the organization (1=not responsible at all - 4=completely responsible), organization size (revenue and number of employees), and IT budget as controls in our research model (Benlian 2009; Hsu et al. 2015). We pre-validated our measurement model in a pretest with 8 MIS researchers by using a cognitive interview technique. The pretest resulted in minor changes to improve the clarity of the model. Our study's final measurement items are shown in Table 20.

**Table 20: Overview of Constructs**

Construct	Items	Source
<b>Perceived risks</b>	How do you evaluate the overall risk (i.e., financial, strategic, security, performance, and management risks) associated with adoption of [in-house / SaaS] applications? (1=not risky at all - 7=extremely risky)	Based on Featherman and Pavlou (2003)
	How do you evaluate the risk that the expected benefits of adopting [in-house / SaaS] applications will not materialize? (1=not risky at all - 7=extremely risky)	
	How do you evaluate the danger that is generally associated with the adoption of [in-house / SaaS] applications? (1=not risky at all - 7=extremely risky)	
<b>Perceived benefits</b>	The overall advantage of adopting [In House / SaaS] applications is... (1=very low - 7=extremely high)	Based on Gewald and Dibbern (2009)
	The potential cost reduction associated with the adoption of [in-house / SaaS] applications is... (1=very low - 7=extremely high)	

	Overall, I consider [in-house / SaaS] adoption to be a useful strategic option. (1=strongly disagree - 7=strongly agree)	
<b>Intention</b>	If there is a superior offer, a SaaS solution should be used for the application domain that I am in charge of. (1=strongly disagree - 7=strongly agree)	Based on Gewald and Dibbern (2009)
	Our company should increase the existing level of adopting SaaS applications. (1=strongly disagree - 7=strongly agree)	
	I support the further adoption of SaaS applications for the application domain that I am in charge of. (1=strongly disagree - 7=strongly agree)	

Our quantitative study was conducted between March 17 and May 1, 2016 in a European country. In a key informant approach, we contacted a total of 1,126 decision makers from organizations of various industries via a contact request on an online social business network. To encourage participation, a management report about the results was offered to the participants. A total of 251 (22.3%) of the 1,126 contacted decision makers agreed to participate in our study and were sent links to access the online survey. One week after sending the invitation, a reminder was sent via another direct message on the social business network. With 131 completed surveys, the response rate was 11.6%. Two main reasons were given for not participating: the contacted decision makers either stated time pressure or that their organizations do not participate in such studies in general. Altogether, 4 of the 131 participants stated to be not responsible for sourcing decisions in their organizations and 4 data sets were identified to have poor data quality. These 8 data sets were excluded from the data analysis, which is therefore based on 123 valid data sets. The sample characteristics can be extracted from Table 21.

In addition to these sample characteristics, we further analyzed the differences within our sample according to the proportion of participating industry sectors and the respective average level of SaaS experience within those sectors. Table 22 shows the proportion of each industry sector relative to the overall sample and the average level of self-reported SaaS experience in each industry (0%=complete absence of SaaS use-100%=all enterprise applications deployed as a service). According to our analysis, most respondents work in IT, Professional Services, and Manufacturing and the highest experience levels are reported by decision makers in Telecommunications, IT, Retail, and Professional Services.

**Table 21: Overview of Sample Characteristics**

Company Size (Number of Employees)		Position	
Small (<50)	36 (29.3%)	CEO	3 (2.4%)
Medium (50-249)	18 (14.6%)	CIO	73 (59.3%)
Corporation (>249)	69 (56.1%)	CTO	20 (16.3%)
Sales p.a.		IT Manager	21 (17.1%)
<1 m EUR	22 (17.9%)	Others	6 (4.9%)
1-9 m EUR	23 (18.7%)	Work Experience	
10-99 m EUR	23 (18.7%)	1-5 years	16 (13.0%)
>99 m EUR	55 (44.7%)	6-10 years	30 (24.4%)
		11 years and more	77 (62.6%)

**Table 22: Segmentation of Industry Sectors**

Industry Sector	Proportion of Total Sample	Average SaaS Experience
Real Estate	0.8%	0 %
Travel & Tourism	0.8%	0 %
Education & Administration	4.1%	1.20 %
Pharmacology & Medical	2.4%	3.33 %
Logistics & Transportation	3.3%	3.75 %
Energy & Utilities	2.4%	5.00 %
Health Care	4.1%	7.00 %
Manufacturing	13.0%	7.06 %
Construction	5.7%	7.14 %
Consumer Goods	2.4%	8.33 %
Financial Services	6.5%	27.00 %
Professional Services	17.1%	34.43 %
Retail & Wholesale	6.5%	37.00 %
IT	22.8%	39.00 %
Telecommunications	4.9%	53.33 %
Others	3.3%	33.75 %

### 6.3.2 *Assessment of Measurement Validations*

The Shapiro-Wilk Test showed that the data is not normally distributed. Furthermore, we calculated the time to respond by considering the number of days between sending access to the online survey to the participants and the actual survey completion to test for non-response bias. Based on that, we compared the data of the first 25% of participants (i.e., shortest time to respond in days) with the last 25% (i.e., longest time to respond in days) (Armstrong and Overton 1977). The Mann-Whitney-U test revealed the non-existence of significant differences. Given that studies using self-report measures to capture dependent and independent variables in the same survey might suffer from common method biases (Podsakoff et al. 2003), we included a marker variable in our survey. The results of the correlation analysis did not indicate significant correlation between the marker variable and the measurement variables. Accordingly, it can be assumed that our data does not suffer from common method bias (Lindell and Whitney 2001).

Due to the explorative nature of our study and the non-normality of our data, we evaluated our research model by using the non-parametric Partial Least Squares (PLS) methodology following the guidelines proposed by Hair et al. (2013). Correspondingly, we first evaluated criteria for discriminant and convergent validity in order to assess our measurement model correctly. Therefore, we extracted parameters for indicator reliability, composite reliability (CR), average variance extracted (AVE) and computed Cronbach's alphas (CA) (see Table 23). With a single exception (indicator 2 of perceived benefits: 0.655), all outer loadings are above the threshold of 0.7. However, all indicator reliability values are larger than the minimum acceptable level of 0.4 and beyond that, most of them are close or above the optimal level of 0.7 (Hulland 1999). The values of composite reliability of all constructs are well-above the threshold level of 0.7, as suggested by Bagozzi and Yi (1988). Regarding AVE, the values of all the constructs exceed the level of 0.5 (Bagozzi and Yi 1988) and the values for Cronbach's alpha, reflecting the internal consistency of the constructs, are also all above the threshold of 0.7 (Nunnally 1978). Moreover, according to Hair et al. (2012)'s recommendation of sample sizes in PLS, a statistical power of 80% is sufficient for a measurement model with a sample size of 123. In summary, the discriminant and convergent validity of our model can be presumed.



**Table 23: Assessment of Measurement Model**

#	Construct	Loadings	Indicator Reliability	CA	CR	Correlation to Construct # / Square Root of AVE [bold]				
						1	2	3	4	5
1	Risks in-house	0.864-0.936	0.746-0.876	0.886	0.929	<b>0.902</b>				
2	Risks SaaS	0.800-0.881	0.640-0.776	0.814	0.888	-0.540	<b>0.852</b>			
3	Benefits in-house	0.706-0.858	0.498-0.736	0.704	0.832	-0.488	0.534	<b>0.790</b>		
4	Benefits SaaS	0.655-0.897	0.429-0.805	0.742	0.850	0.471	-0.605	-0.439	<b>0.811</b>	
5	Intention SaaS	0.885-0.960	0.783-0.904	0.925	0.952	0.540	-0.727	-0.522	0.720	<b>0.932</b>

The Fornell-Larcker Criterion Analysis for checking discriminant validity (Fornell and Larcker 1981) showed that the square root of the AVEs of each construct (highlighted bold) is greater than the correlations among the construct with any other construct in the model (see Table 23). In sum, it can be concluded that our measurement model is well-specified.

To test for multicollinearity, we calculated the Variance Inflation Factor (VIF) values. The VIFs values (Risks in-house=1.313, Risks SaaS=1.903, Benefits in-house=1.313, Benefits SaaS=1.749) are all below 5 (Hair et al. 2011). Thus, we can exclude collinearity problems for our model.

### 6.3.3 Data Analysis and Results

In order to test our hypotheses, we chose a two-step data analysis approach (see Figure 12). In the first step, we test our research model regarding the influence of reference points (attitudinal beliefs about incumbent in-house systems) on the perception of risks and benefits associated with SaaS (attitudinal beliefs about SaaS) (H1a and H1b) as well as the resulting intention to adopt SaaS (H2a and H2b). In the second step, we utilized a multi-group analysis (MGA) for analyzing whether the influence of reference points is moderated by the existing experience with SaaS applications.

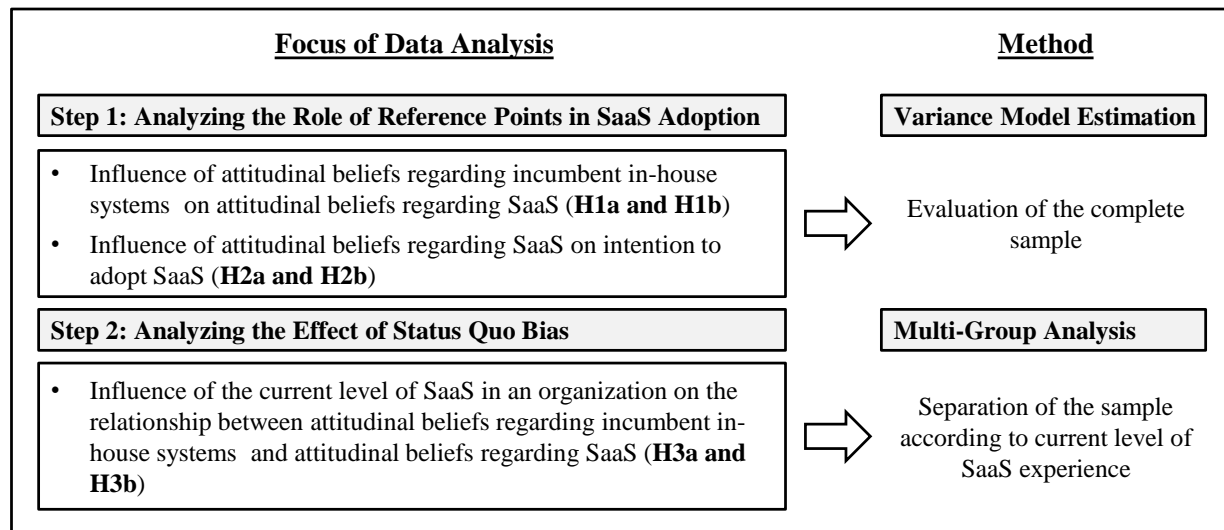


Figure 12: Data Analysis

#### 6.3.3.1 Step 1: The Role of Reference Points in SaaS Adoption

To test our hypotheses H1a and H1b as well as H2a and H2b, the effect sizes and significance of path coefficients were evaluated based on a PLS algorithm and a bootstrapping procedure (5,000 samples, no sign change option, mean replacement). The results are shown in Table 24.

We found that the perceived benefits of in-house systems are significantly negatively associated with the perceived benefits of SaaS ( $\beta = -0.451$ ,  $p < 0.001$ ), supporting H1a. The negative relationship between the perceived risks of in-house systems and perceived risks of SaaS is also identified to be significant ( $\beta = -0.545$ ,  $p < 0.001$ ), supporting H1b. Regarding H2a we found that the positive association of perceived benefits of SaaS with the intention to adopt SaaS is significant ( $\beta = 0.439$ ,  $p < 0.001$ ). Thus, H2a is supported. Moreover, our analysis showed that the negative association of the perceived risks of SaaS with the intention to adopt SaaS is significant ( $\beta = -0.462$ ,  $p < 0.001$ ). Accordingly, H2b is supported as well.

Following the bootstrapping-based approach of Preacher and Hayes (2008), we found that a significant indirect effect of the perceived benefits of in-house systems on the intention to adopt SaaS through the perceived benefits of SaaS is  $-0.198$  ( $p = 0.006$ ). The size of the indirect effect of the perceived risks of in-house systems on intention to adopt SaaS through the perceived risks of SaaS is significant with an indirect effect size of  $0.252$  ( $p = 0.002$ ).

In sum, the results show that our model explains 70.2% of variance in the intention to adopt SaaS ( $R^2 = 0.702$ ), 29.7% of the variance in perceived benefits of SaaS ( $R^2 = 0.297$ ), and 20.3% of the variance in the perceived risks of SaaS ( $R^2 = 0.203$ ).

**Table 24: Results of the Variance Model Estimation**

Relationship	Path Coefficients	Results
Perceived benefits of in-house systems → perceived benefits of SaaS	-0.451***	<i>H1a supported</i>
Perceived risks of in-house systems → perceived risks of SaaS	-0.545***	<i>H1b supported</i>
Perceived benefits of SaaS → intention to adopt SaaS level	0.439***	<i>H2a supported</i>
Perceived risks of SaaS → intention to adopt SaaS	-0.462***	<i>H2b supported</i>
Significance level: *** $p < 0.001$		

There was no significant influence of the control variables (work experience:  $\beta=0.059$ ,  $p=0.427$ ; number of decisions:  $\beta=0.009$ ,  $p=0.722$ ; self-stated responsibility for sourcing decisions:  $\beta=-0.021$ ,  $p=0.512$ ; revenue:  $\beta=0.025$ ,  $p=0.598$ ; size:  $\beta=-0.031$ ,  $p=0.477$ ; IT budget:  $\beta=0.069$ ,  $p=0.439$ ).

#### 6.3.3.2 Step 2: The Effect of Status Quo Bias on Attitudinal Beliefs Regarding SaaS

In order to test H3a and H3b, we had to perform a multi-group analysis (MGA) procedure (e.g., Hair et al. 2011; Sarstedt et al. 2011). Accordingly, we separated our data set into two groups: organizations currently maintaining almost all of their enterprise applications in-house (i.e., organizations with no or a low SaaS level) and organizations that already utilize a substantial degree of SaaS (i.e., organizations with a medium or high SaaS level). We split the data sets at a marginal level of SaaS use of 5% in an organization. Accordingly, organizations that still host more than 95% of their enterprise applications in-house ( $n=39$ ) are considered to have less experience with the new technology, thus, face a higher level of uncertainty when making decisions about future SaaS usage. On the other hand, organizations that already use 5% or more of their enterprise applications as a service ( $n=84$ ) are assigned to the group that is expected to have a certain degree of experience with SaaS and, therefore, will base the adoption decision less on reference points (attitudinal beliefs about in-house systems). The results of the MGA are shown in Table 25. These results show that all of the hypothesized relationships in H1 and H2 are significant for both organizations with no or low SaaS experience and organizations with medium or high SaaS experience. However, the path coefficients of the relationships between perceived benefits and risks of in-house systems and

perceived benefits and risks of SaaS are found to be significantly different with respect to the differences in experience with SaaS. Specifically, the negative influence of perceived benefits of in-house systems on the perceived benefits of SaaS is significantly higher for organizations that have no or low SaaS experience ( $\beta=-0.640$ ;  $p<0.001$ ) than for organizations that have medium or high SaaS experience ( $\beta=-0.379$ ;  $p=0.008$ ; MGA  $p=0.029$ ). Accordingly, H3a is supported. Regarding the relationship between the perceived risks of in-house systems and perceived risks of SaaS, significant differences were found as well (MGA  $p=0.017$ ). As such, the negative relationship between the perceived risks of in-house systems and perceived risks of SaaS is significantly higher for organizations with no or low experience with SaaS ( $\beta=-0.728$ ;  $p<0.001$ ) than for organizations with a medium or high level of experience with SaaS ( $\beta=-0.445$ ;  $p=0.001$ ). Therefore, H3b is supported. Differences between the two groups of organizations regarding the influence of perceived benefits and risks of SaaS on the intention to adopt SaaS were not found.

**Table 25: Results of the Multi-Group Analysis**

Relationship	Path Coefficients		p-value of Multi-Group Analysis	Results
	Low or No SaaS Experience (n=39)	Medium or High SaaS Experience (n=84)		
Perceived benefits of in-house systems $\rightarrow$ perceived benefits of SaaS	-0.640***	-0.379***	0.029	<i>H3a supported</i> : stronger for organizations with no or low SaaS experience
Perceived risks of in-house systems $\rightarrow$ perceived risks of SaaS	-0.728***	-0.445***	0.017	<i>H3b supported</i> : stronger for organizations with no or low SaaS experience
Significance level: *** $p < 0.001$				

## 6.4 Discussion

Previous research has repeatedly highlighted the importance of perceived risks and benefits in organizational service innovation adoption (e.g., Benlian and Hess 2011; Featherman and Pavlou 2003; Wu et al. 2011). However, when analyzing decisions about replacing incumbent technologies with new technologies, it is essential to consider the complexity along with the high degree of uncertainty due to a lack of experience surrounding such decisions. Confronted

with decision making under uncertainty, individuals often rely on cognitive “shortcuts”, i.e., the dependence on reference points in a particular decision-making process (Shoham and Fiegenbaum 2002). In the context of a replacement decision of an existing in-house technology with a new technology, decision makers encounter a lack of information because of lacking experience or absent historical data that induces such cognitive shortcuts. On account of this, we developed a research model that demonstrates the influence of incumbent technologies (i.e., in-house systems) on the assessment of attitudinal beliefs (i.e., perceived benefits and risks) regarding SaaS on the basis of Prospect Theory and Status Quo Bias research. In a two-step analysis, based on the data of a large scale empirical study with decision makers who are responsible for the organizational IT, we (1) identified the significant influence of reference-dependence affecting the rational weighing up of risks and benefits associated with a new SaaS technology and (2) measured the effect of the Status Quo Bias depending on the already acquired experience level of SaaS use.

We discovered that decision makers' assessments of a new SaaS technology are negatively influenced by their attitude toward the incumbent technology. In other words, if decision makers consider their incumbent system to be satisfactory because the perceived benefits outweigh the perceived risks, they will tend to form a rather negative attitude toward new, unfamiliar SaaS technologies. Vice versa, decision makers that, for example, already experienced security incidents with their incumbent technology and thus perceive higher risks associated with existing in-house solutions, will more likely display a positive attitude toward SaaS. Accordingly, decision makers who realized that their incumbent system does not offer financial benefits (any longer) will be more receptive of potential cost reductions offered by a SaaS solution and therefore, perceive benefits of SaaS higher. To conclude, the incumbent technology can exert a pronounced influence on the final SaaS adoption decision.

In addition, our results illustrate that the dependence on reference points differs significantly according to the SaaS experience in the respective organization. In contrast to previous research (Vetter et al. 2011), we are not measuring self-stated experience with SaaS according to Dibbern (2004) or Roodhooft and Warlop (1999), but rather control our study for this relationship with a defined moderator variable called SaaS experience for objective measurement. We were able to demonstrate a stronger influence of the Status Quo Bias in organizations with little to no SaaS experience. Especially, less experienced decision makers will regard the retention of the Status Quo as less risky compared to the potentially negative consequences of an adoption or replacement decision. This inaccurate assessment of risks can

be regarded as a result of loss aversion, i.e., the overestimation of perceived risks of the SaaS solution. For example, decision makers could overestimate the probability and the actual consequences of down-time issues and will assess this risk more severely compared to the current risks of their incumbent system. Thus, without the necessary knowledge and past experience, a deviation from the incumbent system will be regarded as an unnecessary risk resulting in the retention of the Status Quo.

Our study offers several theoretical and practical implications. We specifically contribute to the stream of technology acceptance research by singling out the importance of reference points and Status Quo Bias in the context of SaaS adoption decisions. In particular, our study is the first using Prospect Theory to analyze decision makers' appraisals of SaaS in an organizational context by considering their evaluation of the incumbent technology they are familiar with. Moreover, our results indicate that Status Quo-Thinking is more pronounced according to the experience level indicating that adoption decisions of service innovations are potentially more affected by Status Quo Bias. Given that new organizational IT systems are almost exclusively replacement decisions, future research should consider the relevance of incumbent systems when devising their study designs. We deliberately chose a research approach based on a very generic risk-benefit assessment which could thus be adjusted according to other scenarios considering adoption, service innovation, or replacement decisions (Lee 1999). In addition, our way of measuring the Status Quo Bias at the group level can contribute to future research as most studies so far measure Status Quo Bias with indicators such as perceived inertia or perceived sunk costs that are predominantly based on self-assessment on an individual level (e.g., Polites and Karahanna 2012).

We also offer insights and contributions for practice. Our results indicate that providers of SaaS technologies need to adapt their business models by altering their communication and sales approach according to the respective group of potential customers. Customer groups which already passed a certain threshold in terms of their SaaS level, suffer from a less pronounced degree of Status Quo Bias and will, therefore, be easier to convince of the relative advantage of SaaS and potentially display a higher intention to adopt further solutions. Hence, providers should intend to further capitalize on their current client base with additional horizontal or vertical integration solutions. Another approach for providers that involves the current client base is customer recommendation programs. Due to the social influence on risk assessment (Lee 2009), recommendations given by existing customers can decrease the level of uncertainty. Especially, non-adopters will demand more facts and examples to realize the

relative advantage of a SaaS solution and, therefore, organized roundtables with SaaS-experienced organizations can help both SaaS providers and unexperienced decision makers to realize financial or strategic advantages. A similar way to decrease the inherent Status Quo Bias is the acquirement of further knowledge gained in workshops, lighthouse projects or extended trial versions to gain more experience with a potential new technology. From an organizational perspective, decision makers can already benefit from our study by acknowledging the influence of reference points and Status Quo-Thinking. In order to arrive at a more objective assessment of risks and benefits of both the incumbent and new technology, organizations should, therefore, encourage roundtables or group discussions. These decision-making processes should also include objective assessors such as consultants to accomplish a more objective and rational evaluation of both their incumbent system as well as a possible new SaaS solution. Furthermore, decision makers might be unaware of the difficulties their employees experience with the incumbent technology and, as a consequence, overestimate the benefits of the existing systems. This may result in a distorted perception of the new technology and, hence, obstruct an optimal adoption or replacement decision. Additional information from various parties in the organizational hierarchy might compensate for this lack of information and support an optimal decision-making process further. Against this backdrop, organizations should also scrutinize if their current company culture might encourage Status Quo-Thinking. Previous research in this context demonstrated that company culture itself can enhance Status Quo-Thinking when decision makers “reflect the imprint of cultural socialization more so than professional experience” (Geletkanycz 1997, p. 615). According to Geletkanycz and Black (2001), a deviation from the Status Quo will be regarded even more as an unnecessary risk that could possibly jeopardize a decision maker's position in those organizations characterized by more hierarchical and traditional cultures. Interestingly, our descriptive analysis indicates indeed that more “traditional” industry sectors seem to be less likely to adopt SaaS. Consequently, organizations and individual decision makers should realize that the Status Quo Bias might actually be an obstacle for achieving certain organizational goals, and therefore encourage processes and measures that minimize Status Quo-Thinking.

## **6.5 Limitations, Future Research, and Conclusion**

As with any research, some limitations of this study merit consideration. First, our study is cross-sectional and static. IT services and systems constantly change entailing new requirements and the perceptions of new as well as incumbent technologies might change

over time. As such, future research could enrich the findings of our study regarding the replacement process by measuring the assessments of different technologies longitudinally. By doing so, factors that address the Status Quo Bias, and especially factors that could quickly change the attitude toward the new technology, could be identified in order to develop appropriate countermeasures. Second, this study focuses on the top echelon's assessments of incumbent and new technologies. Even if these decision makers are ultimately responsible for the sourcing decisions in their organizations, IT decisions are often made by groups and may also be influenced by other organizational stakeholders (e.g., customers or investors). Future research can supplement our results by conducting case studies and expert interviews with decision makers at different hierarchical levels in order to fully capture the technology replacement process in organizations. In addition, the results of this study need to be verified within the context of other decisions about organizational technology adoption and in different cultural and legal settings. Decision makers in US companies or in more traditional industry sectors might display different perceptions and attitudes or draw on different reference points due to divergent company cultures than those in Europe, Asia or innovative and service-oriented industries. By way of example, a future study directed primarily at start-ups that are faced with green-field adoptions could analyze whether the attitude toward SaaS is influenced by different reference points (e.g., experience with a technology in a previous organization or recent news about security breaches). Another recommendation for future research would, therefore, encompass experiments to verify our results and to test for other effects, such as further cognitive biases in the organizational decision-making process.

To sum up, our study enhances the understanding of an organization's acceptance of SaaS technologies in particular and replacement decisions in general. When decision makers are confronted with a new technology, they frequently encounter a lack or insufficiency of data and experience. As this is often the case when assessing SaaS technologies, decision makers will draw on their experience with familiar technologies and evaluate the new technology based on their assessment of the existing one. It is essential for SaaS providers to acknowledge this relationship as they risk losing potential selling opportunities if they neglect to frame their sales strategy and marketing efforts according to these cognitive decision-making processes. Correspondingly, decision makers in organizations should be aware that their assessments of risks and the benefits associated with the incumbent technology may be skewed due to Status Quo-Thinking, which in turn, may discourage their organizations from adopting a more efficient technology and inhibiting service innovations in general. Neglecting



to acknowledge these findings could have far-reaching negative consequences for overall organizational performance.

## 7 Summary of Key Findings and Thesis Conclusion

Today, IT security risks are omnipresent in our private and professional life. The extensive usage of IT greatly challenges society to effectively protect data and IT systems from IT security incidents. However, although a large number of various IT security safeguards are available, private individuals and organizations often refrain from adopting those measures that would increase their IT security levels. Against this background, the overarching objective of this thesis was to gain a better understanding about how IT security is perceived by private individuals and managers in organizations and how these perceptions influence protection behaviors. Specifically, the following research objectives were in focus:

- Analyzing gender differences in IT security appraisals and the protective behaviors of private individuals (chapter 3)
- Developing a conceptualization of top managers' IT security awareness (chapter 4)
- Analyzing managers' WTP for IT security safeguards (chapter 5)
- Analyzing managers' Status Quo-Thinking (chapter 6)

### 7.1 Theoretical Implications

Overall, the findings across the four research papers included in this thesis contribute to IS research in the field of IT security by advancing our understanding of IT security perceptions and the protective behaviors of private individuals and managers in organizations. Within the four studies presented in chapters 3 to 6, the different perspectives on IT security are taken within the private context and business context. As — depending on the research questions — these studies draw on different literature streams, the main theoretical implications that can be derived from the studies in this thesis will be separately discussed in the following.

Regarding IT security perceptions and the protective behaviors of private individuals (research paper A, chapter 3), we extended existing IS research by being the first to examine the role of individuals gender. The results show that females and males base their perceptions on different cognitive processes and therefore, their protective behaviors are influenced by

different factors. These gender differences in threat and coping appraisals are important to be contemplated in future research since they may explain inconsistencies in findings across previous IS studies on IT security perceptions. When analyzing the compliance behavior of employees within the business context, gender differences may be of similar relevance. If females' threat and coping appraisals are based on different cognitive processes than males' threat and coping appraisals, the information given within SETA programs may have a different impact on the compliance behavior of males and females.

Furthermore, we contribute to existing IS research by not only analyzing the IT security perceptions and stated intentions of the participants but also their actual protection behavior. The conducted behavioral experiments and supplementary interviews showed that a significant positive relationship between the stated intentions and the actual protection behaviors only exists within the female sample but not within the male sample. Males seem to be less likely to translate their protection intention into actual behavior than females. Future research should build on the results of this study and further analyze possible reasons for this intention-behavior gap (see e.g., Sheeran 2002) across males.

Within the business context, the study presented in research paper B (chapter 4) highlights and confirms the crucial role of top managers for effective IT security management in organizations as assumed in previous research (e.g., Ashenden 2008; Sharma and Yetton 2007). By drawing on a structured literature review and qualitative expert interviews, an exhaustive conceptualization of top managers' IT security awareness — comprising both individual as well as organizational factors — is developed and tested. This conceptualization serves as a fundamental basis for future research to better understand the formation of organizational IT security investment decisions. For example, previous studies indicate that although managers might show concerns regarding the IT security of their organizational IT systems, their actual IT security behavior might not be appropriate (i.e., low IT security investments). The developed conceptualization of top managers' IT security awareness may enable future IS research to explain this paradoxical attitude-behavior gap. Furthermore, the results indicate, that for effective IT security management, not only top managers' IT security awareness is crucial but also the IT security awareness of department managers. Built on that, future studies should intensify the research on managers' IT security awareness and thereby consider all the hierarchical levels of an organization. The future studies should also analyze whether and to what degree differences regarding the concept of IT security awareness across the different hierarchical levels exist.

The study in research paper C (chapter 5) highlights the necessity to consider that the implementation of IT security safeguards is not only associated with advantages (e.g., risk reduction) but can be also associated with disadvantages (e.g., performance reduction). The findings show that IT security safeguards are differently evaluated by different managers in various organizations and that these different evaluations determine their WTP for the respective measure. To the best of our knowledge, this study is the first adapting Kano's Theory (Kano et al. 1984) to the IT security context. It is demonstrated that both positive (functional) characteristics and negative (dysfunctional) characteristics of IT security safeguards are relevant when analyzing managers' WTP and adoption decisions. As such, the results enable researchers to better understand and predict the outcome of IT security management decisions by considering IT security safeguard evaluation in terms of five IT security safeguard categories: basic, performance, advanced, indifferent, and reverse IT security safeguards. Considering this multidimensional nature of the evaluation of IT security safeguards might also allow future research to reinvestigate yet unclear behavioral phenomena like people refraining from adopting safeguarding measures even when they perceive the addressed risks to be very critical (e.g., Johnston and Warkentin 2010). Furthermore, the results are also relevant for future research in mathematical IT security optimization models.

Research paper D (chapter 6) also comes with several important theoretical implications. The results demonstrate that when managers are confronted with decision making under uncertainty, they frequently rely on cognitive "shortcuts": Their risk and benefit assessments regarding a new technology are significantly influenced by reference points (Shoham and Fiegenbaum 2002). These reference points are given by the perceived benefits and risks of the currently used technology (the Status Quo) and have an even stronger influence the less experienced a manager is with the new technology. In particular, it is found that managers' decisions to adopt a new SaaS technology is strongly influenced by the perceived risks and benefits associated with an existing in-house solution. As a consequence, when a manager perceives the existing IT solution as being associated with low risk, the perceived risk of a new technology will be automatically higher — even though the new technology actually brings more benefits and less risks. As such, the study contributes to the stream of technology acceptance research by singling out the importance of reference points and Status Quo Bias. Since previous IS research found that IT security risks are the dominant factor influencing managers' overall risk perception of SaaS adoption (e.g., Benlian and Hess 2011), it can be concluded that the evaluation of perceived IT security risks will be most probably also

affected by Status Quo-Thinking. Future research can build on our findings by considering the role of reference points and a possible Status Quo Bias in IT security risk perception when analyzing managers' decisions to adopt IT security safeguards.

In sum, this thesis provides substantial theoretical implications with empirical evidence to the emerging body of research on IT security perceptions and behaviors. It is demonstrated that — in both the private and the business context — IT security perceptions and behaviors are multifaceted and highly complex in nature. Therefore, many research questions remain unanswered and behavioral phenomena are far from being well understood. By conducting multiple research studies, we advance the existing research on IT security perceptions and behaviors of private individuals and managers in organizations, provide a basis for future studies, and hope to encourage future researchers to further validate and analyze our findings in other settings.

## **7.2 Practical Implications**

Besides the theoretical implications, a number of practical implications and recommendations can be derived from the studies in this thesis. In particular, private individuals, managers in organizations, and suppliers of IT and IT security products benefit from our results. Again, the main practical implications of the four studies will be consecutively presented.

Research paper A (chapter 3) shows that female and male smartphone users evaluate IT security risks differently and that they also differ in their protective behavior. Specifically, our results indicate that, during risk assessment, female users only consider the severity that would result from a risk, while male users also take the probability of becoming a victim into consideration. Therefore, female users might evaluate risks that are associated with less damage but are very likely to happen to be lower than IT security risks that are extremely unlikely to happen but would come along with far-reaching consequences. Female users should strive to assess risks more rationally by also considering the probability of the negative event in order to avoid possible underestimations of risks that they are highly susceptible to — even though the associated damage seems to be somehow manageable. On the other side, our results show that male users should be aware that they tend to not necessarily behave as securely as they originally intended. We only found a significant positive relationship between stated intentions and actual protection behaviors within the female sample but not within the male sample. Overall, it is demonstrated that private users should carefully consider on which factors their threat and coping appraisals are based on and whether the

safeguarding measures that they have taken for their mobile devices are adequate. Furthermore, organizations as well as suppliers of IT security products can also benefit from the findings. Specifically, since females and males are found to base their threat and coping appraisals on different cognitive processes, organizations can use the results of this study when developing and revising security, education, training, and awareness (SETA) programs. Similarly, suppliers of IT security products should consider our results when developing marketing campaigns and strategies.

The first study conducted within the business context (research paper B, chapter 4) clearly showed that for ensuring a high level of IT security, organizations should not only focus on IT security awareness at the employee level but also at the management level. Of course, a high level of IT security awareness among employees is in fact highly relevant. Nevertheless, managers' awareness about IT security is at least of similar importance and, therefore, should not be neglected. A lack of IT security awareness of top and/or department managers can result in insufficient scope for action of the organizations' IT security specialists (i.e., financial resources, human resources, and flexibility in decision-making) and in turn, threaten the organization's data and IT systems. Our results show that the combination of decision-power and IT security awareness is crucial for effective IT security management. Thus, to ensure an adequate IT security level within an organization, appropriate positions must be identified and integrated in the organizational structure. Moreover, since we identified individual and organizational factors that together build the concept of top managers' IT security awareness, the results are also helpful when developing educational programs specifically for managers with decision-power regarding the organizational IT security management.

The results of our second study within the business context (research paper C, chapter 5) are especially beneficial for suppliers of IT security products as well as for IT suppliers. Suppliers of IT security products can analyze to what degree their products are differently evaluated by their customers and thereby identify relevant customer groups with different IT security requirements and different levels of WTP. Based on that, product development, pricing strategies, and marketing strategies can be optimized. Suppliers of IT products can analyze how the safeguards implemented in their IT products influence their customers' satisfaction and, therefore, their associated WTP. By doing so, they can effectively allocate development resources by identifying which safeguards should be implemented, improved, or removed from a certain IT product. Overall, the results highlight that IT (security) suppliers should

carefully consider their customers' individual IT security needs in order to derive effective strategies and thereby to gain economic and competitive advantages.

Finally, important practical implications can be derived from the findings of the third study conducted among managers within the business context (research paper D, chapter 6). We found that managers are prone to Status Quo-Thinking and that the resulting Status Quo Bias is larger the less experienced a manager is with a new technology. From the perspective of suppliers of IT and IT security products, it may, therefore, be beneficial to categorize customer groups with respect to different levels of experience. Based on that, sales and communication approaches can be accordingly adapted. Moreover, from the perspective of managers in customer organizations, the results highlight the importance of roundtables, expert groups, and extended trial versions to create a reliable basis of knowledge and experience and thus, to avoid Status Quo Bias when deciding to adopt a new IT (security) product. In addition, especially when IT security knowledge and experience is generally very low within an organization, objective assessors during evaluation and decision-making processes might be necessary to ensure that the best decision for the organization is made.

In conclusion, this thesis provides a further step toward an understanding of the risk perceptions and protective behaviors of private individuals and managers in organizations. In summary, the findings provide helpful recommendations to private individuals and managers in organizations on how to improve their protection behaviors, and the suppliers of IT and IT security products on how to better understand their customers' needs and thereby gain economic and competitive advantages. Nevertheless, future research should use our work as a basis for supplementary analysis and verifications, and to further advance our knowledge about IT security perceptions and behaviors.

## References

- Abdul Talib, Y., and Dhillon, G. 2015. "Employee ISP Compliance Intentions: An Empirical Test of Empowerment," in *Proceedings of the 36th International Conference of Information Systems (ICIS)*, Fort Worth, USA, p. 13.
- Ackermann, T., Widjaja, T., Benlian, A., and Buxmann, P. 2012. "Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development," in *Proceedings of the 33rd International Conference on Information Systems (ICIS)*, Orlando, USA, p. 3.
- Acquisti, A., and Grossklags, J. 2004. "Privacy Attitudes and Privacy Behavior," in *Economics of Information Security*, L.J. Camp and S. Lewis (eds.). Boston, USA: Springer, pp. 165-178.
- Ajzen, I. 1985. *From Intentions to Actions: A Theory of Planned Behavior*. Berlin/Heidelberg, Germany: Springer.
- Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.
- Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behaviours*. Eaglewood Cliffs, USA: Prentice Hall.
- Albrechtsen, E., and Hovden, J. 2010. "Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection – An Intervention Study," *Computers & Security* (29:4), pp. 432-445.
- Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.
- Anderson, E. W. 1996. "Customer Satisfaction and Price Tolerance," *Marketing Letters* (7:3), pp. 265-274.



- Armstrong, J. S., and Overton, T. S. 1977. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14:3), pp. 396-402.
- Ashenden, D. 2008. "Information Security Management: A Human Challenge?," *Information Security Technical Report* (13:4), pp. 195-201.
- AVAST 2014. "New AVAST Survey Shows People Not So Smart with Smartphone Security." <https://blog.avast.com/2014/04/07/new-avast-survey-shows-people-not-so-smart-with-smartphone-security/>. Accessed 07/05/2016.
- Avižienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. 2004. "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing* (1:1), pp. 11-33.
- Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., and Chai, S. 2010. "Women in Cybersecurity: A Study of Career Advancement," *IT Professional* (12:1), pp. 24-31.
- Bagozzi, R. P., and Yi, Y. 1988. "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science* (16:1), pp. 74-94.
- Bamberger, P., and Fiegenbaum, A. 1996. "The Role of Strategic Reference Points in Explaining the Nature and Consequences of Human Resource Strategy," *Academy of Management Review* (21:4), pp. 926-958.
- Bansal, G., Hodorff, K., and Marshall, K. 2016. "Moral Beliefs and Organizational Information Security Policy Compliance: The Role of Gender," in *Proceedings of the Eleventh Midwest United States Association for Information Systems*, Milwaukee, USA, p. 11.
- Bansal, G., and Shin, S. I. 2016. "Interaction Effect of Gender and Neutralization Techniques on Information Security Policy Compliance: An Ethical Perspective," in *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, USA, p. 32.
- Barclay, D., Higgins, C., and Thompson, R. 1995. "The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," *Technology Studies* (2:2), pp. 285-309.
- Barnett, R. C., and Marshall, N. L. 1991. "The Relationship Between Women's Work and Family Roles and Their Subjective Well-Being and Psychological Distress," in *Women, Work, and Health - Stress and Opportunities*, M. Frankenhaeuser, U. Lundberg and M. Chesney (eds.). New York, USA: Springer, pp. 111-136.

- Bazerman, M. H., and Moore, D. A. 2008. *Judgement in Managerial Decision Making*. New York, USA: Wiley.
- BBC 2014. "Sony Pictures Computer System Hacked in Online Attack." <http://www.bbc.com/news/technology-30189029>. Accessed 12/13/2017.
- Bedner, M., and Ackermann, T. 2010. "Schutzziele der IT-Sicherheit," *Datenschutz und Datensicherheit* (34:5), pp. 323-328.
- Belanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11:3), pp. 245-270.
- Bem, S. L. 1981. "Gender Schema Theory: A Cognitive Account of Sex Typing," *Psychological Review* (88:4), pp. 354-364.
- Benlian, A. 2009. "A Transaction Cost Theoretical Analysis of Software-as-a-Service (SAAS)-based Sourcing in SMBs and Enterprises," in *Proceedings of the 17th European Conference in Information Systems (ECIS)*, Verona, Italy, p. 4.
- Benlian, A., and Hess, T. 2010. "The Risks of Sourcing Software as a Service-An Empirical Analysis of Adopters and Non-Adopters," in *Proceedings of the 18th European Conference on Information Systems (ECIS)*, Pretoria, South-Africa, p. 142.
- Benlian, A., and Hess, T. 2011. "Opportunities and Risks of Software-as-a-Service: Findings from a Survey of IT Executives," *Decision Support Systems* (52:1), pp. 232-246.
- Benlian, A., Hess, T., and Buxmann, P. 2009. "Drivers of SaaS-Adoption – An Empirical Study of Different Application Types," *Business & Information Systems Engineering* (1:5), pp. 357-369.
- Berger, C., Blauth, R., Boger, D., Bolster, C., Burchill, G., DuMouchel, W., Pouliot, F., Richter, R., Rubinoff, A., Shen, D., Timko, M., and Walden, D. 1993. "Kano's Methods for Understanding Customer-Defined Quality," *Center for Quality of Management Journal* (2:4), pp. 1-37.
- Bettman, J. R. 1973. "Perceived Risk and Its Components: A Model and Empirical Test," *Journal of Marketing Research* (10:2), pp. 184-190.
- Bhattacharyya, S., and Rahman, Z. 2004. "Capturing the Customer's Voice, the Centerpiece of Strategy Making: A Case Study in Banking," *European Business Review* (16:2), pp. 128-138.

- Bhattacharjee, A., and Sanford, C. 2006. "Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model," *MIS Quarterly* (30:4), pp. 805-825.
- Blackwell, E. 1998. "Building a Solid Foundation for Intranet Security," *Information Systems Management* (15:2), pp. 26-33.
- Boni, B. 2000. "Meteors and Managers," *Network Security* (2000:11), pp. 18-19.
- Bornstein, R. F. 1989. "Exposure and Affect: Overview and Meta-Analysis of Research, 1968-1987," *Psychological Bulletin* (106:2), pp. 265-289.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837-864.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.
- Bozionelos, N. 1996. "Psychology of Computer Use: XXXIX. Prevalence of Computer Anxiety in British Managers and Professionals," *Psychological Reports* (78:3), pp. 995-1002.
- Brown, S. R. 1986. "Q Technique and Method: Principles and Procedures," in *New Tools for Social Scientists: Advances and Applications in Research Methods*, W.D. Berry and M. Lewis-Beck (eds.). Beverly Hills, USA: SAGE Publications, pp. 57-76.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.
- Buss, D. M. 1988. "The Evolution of Human Intrasexual Competition: Tactics of Mate Attraction," *Journal of Personality and Social Psychology* (54:4), p. 616.
- Byrnes, J. P., Miller, D. C., and Schafer, W. D. 1999. "Gender Differences in Risk Taking: A Meta-Analysis," *Psychological Bulletin* (125:3), pp. 367-383.
- Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. 2015. "Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources," *Information & Management* (52:4), pp. 385-400.

- Cavusoglu, H., Cavusoglu, H., and Zhang, J. 2008. "Security Patch Management: Share the Burden or Share the Damage?," *Management Science* (54:4), pp. 657-670.
- Charmaz, K. 2014. *Constructing Grounded Theory*. London, United Kingdom: SAGE Publications.
- Chau, P. Y. K. 1996. "An Empirical Assessment of a Modified Technology Acceptance Model," *Journal of Management Information Systems* (13:2), pp. 185-204.
- Chen, C. C., Shaw, R., and Yang, S. C. 2006. "Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System," *Information Technology, Learning, and Performance Journal* (24:1), pp. 1-14.
- Choi, N., Kim, D., and Goo, J. 2006. "Managerial Information Security Awareness' Impact on an Organization's Information Security Performance," in *Proceedings of the 12th Americas Conference on Information Systems (AMCIS)*, Acapulco, Mexico, pp. 3367-3375.
- Choi, N., Kim, D., Goo, J., and Whitmore, A. 2008. "Knowing Is Doing: An Empirical Validation of the Relationship Between Managerial Information Security Awareness and Action," *Information Management & Computer Security* (16:5), pp. 484-501.
- Cisco 2016. "Cisco Global Cloud Index: Forecast and Methodology, 2015–2020." <http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf>. Accessed 11/11/2016.
- Clegg, B., Wang, T., and Ji, P. 2010. "Understanding Customer Needs Through Quantitative Analysis of Kano's Model," *International Journal of Quality & Reliability Management* (27:2), pp. 173-184.
- Cline, M., and Jensen, B. 2004. "Information Security: An Organizational Change Perspective," in *Proceedings of the 10th Americas Conference on Information Systems (AMCIS)*, New York, USA, pp. 4514-4520.
- Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.
- Cranor, L. F., and Garfinkel, S. 2005. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc.

- Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, (4th ed.). Thousand Oaks, USA: Sage Publications.
- Cybersecurity Ventures 2016. "Hackerpocalypse: A Cybercrime Revelation." <http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Accessed 05/03/2017.
- D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.
- Dahlberg, T., Kivijärvi, H., and Saarinen, T. 2017. "Longitudinal Study on the Expectations of Cloud Computing Benefits and an Integrative Multilevel Model for Understanding Cloud Computing Performance," in *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS)*, Waikoloa, HI, USA, pp. 4251-4260.
- Dang, D., and Nkhoma, M. 2013. "Information Availability as Driver of Information Security Investments: A Systematic Review Approach," in *Proceedings of the 4th International Conference on Information Systems Management & Evaluation*, Ho Chi Minh City, Vietnam, pp. 71-80.
- David, P. A. 1985. "Clio and the Economics of QWERTY," *The American Economic Review* (75:2), pp. 332-337.
- Davis, F. D. 1986. "A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results." Massachusetts Institute of Technology, Sloan School of Management.
- Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319-340.
- Dey, I. 2003. *Qualitative Data Analysis: A User Friendly Guide for Social Scientists*. London, United Kingdom: Routledge.
- Dias, C. S., Cruz, J. F. A., and Fonseca, A. M. 2010. "Coping Strategies, Multidimensional Competitive Anxiety and Cognitive Threat Appraisal: Differences across Sex, Age and Type of Sport," *Serbian Journal of Sports Sciences* (4:1), pp. 23-31.
- Dibbern, J. 2004. *The Sourcing of Application Software Services. Empirical Evidence of Cultural, Industry and Functional Differences*. Heidelberg, Germany: Physica-Verlag.

- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Codel for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.
- Doherty, N. F., and Fulford, H. 2006. "Aligning the Information Security Policy with the Strategic Information Systems Plan," *Computers & Security* (25:1), pp. 55-63.
- Dojkovski, S., Lichtenstein, S., and Warren, M. 2010. "Enabling Information Security Culture: Influences and Challenges for Australian SMEs," in *Proceedings of the 21st Australasian Conference on Information Systems*, Brisbane, Australia, p. 61.
- Dutta, A., and McCrohan, K. 2002. "Management's Role in Information Security in a Cyber Economy," *California Management Review* (45:1), pp. 67-87.
- Eagly, A. H., and Wood, W. 1991. "Explaining Sex Differences in Social Behavior: A Meta-Analytic Perspective," *Personality and Social Psychology Bulletin* (17:3), pp. 306-315.
- Eduserv 2015. "Government, Technology and the Language of Business Change." <https://www.chest.ac.uk/~media/Insight/Reports/WEB1490%20Government%20technology%20and%20the%20language%20of%20business%20change.pdf>. Accessed 11/11/2016.
- EMC 2014. "Downtime and Data Loss Cost Enterprises \$1.7 Trillion Per Year." <http://www.securityweek.com/downtime-and-data-loss-cost-enterprises-17-trillion-year-emc>. Accessed 06/08/2015.
- Eurostat 2014. "Cloud Computing Services Used by One Out of Every Five Enterprises in the EU28." <http://ec.europa.eu/eurostat/documents/2995521/6208098/4-09122014-AP-EN.pdf>. Accessed 11/11/2016.
- Eurostat 2016. "Cloud Computing — Statistics on the Use by Enterprises." [http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud\\_computing\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_statistics_on_the_use_by_enterprises). Accessed 14/04/2017.
- Featherman, M. F., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451-474.
- Festinger, L. 1954. "A Theory of Social Comparison Processes," *Human Relations* (7:2), pp. 117-140.

- Fiegenbaum, A., Hart, S., and Schendel, D. 1996. "Strategic Reference Point Theory," *Strategic Management Journal* (17:2), pp. 219-235.
- Fishbein, M., and Ajzen, I. 1975. *Belief, Attitudes, Intention, and Behavior - An Introduction to Theory and Research*. Reading, USA: Addison-Wesley.
- Fleischmann, M., Amirpur, M., Benlian, A., and Hess, T. 2014. "Cognitive Biases in Information Systems Research: A Scientometric Analysis," in *Proceedings of the 22nd European Conference on Information Systems (ECIS)*, Tel Aviv, Israel, p. 5.
- Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.
- Forbes 2014. "iCloud Data Breach: Hacking And Celebrity Photos." <https://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/#33f059e62de7>. Accessed 12/13/2017.
- Forbes 2015a. "IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'." <https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#5054cfbf73f0>. Accessed 05/03/2017.
- Forbes 2015b. "The IRS Could Have Prevented Its Latest Data Hack. Time For Some TFA." [https://www.forbes.com/sites/kurtmarko/2015/05/27/irs-hack\\_fido-leadership/#264245f8104c](https://www.forbes.com/sites/kurtmarko/2015/05/27/irs-hack_fido-leadership/#264245f8104c). Accessed 05/03/2017.
- Forbes 2016. "Cyber Crime Costs Projected To Reach \$2 Trillion by 2019." <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4a7c85ce3a91>. Accessed 11/23/2017.
- Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.
- Forte, D. 2008. "Selling Security to Top Management," *Network Security* (2008:3), pp. 18-20.
- Franke, G. R., Crown, D. F., and Spake, D. F. 1997. "Gender Differences in Ethical Perceptions of Business Practices: a Social Role Theory Perspective," *Journal of Applied Psychology* (82:6), p. 920.

- Fried, L. 1994. "Information Security and New Technology Potential Threats and Solutions," *Information System Management* (11:3), pp. 57-63.
- Fry, R. B., and Prentice-Dunn, S. 2005. "Effects of Coping Information and Value Affirmation on Responses to a Perceived Health Threat," *Health Communication* (17:2), pp. 133-147.
- Fujita, F., Diener, E., and Sandvik, E. 1991. "Gender Differences in Negative Affect and Well-Being: the Case for Emotional Intensity," *Journal of Personality and Social Psychology* (61:3), pp. 427-434.
- Gal, I. 1996. "Understanding Repeated Simple Choices," *Thinking & Reasoning* (2:1), pp. 81-98.
- Gartner 2014. "Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration." <http://www.gartner.com/newsroom/id/2753017>. Accessed 04/19/2016.
- Gartner 2016. "Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach \$204 Billion in 2016." <http://www.gartner.com/newsroom/id/3188817>. Accessed 11/04/2017.
- Geletkanycz, M. A. 1997. "The Salience of 'Culture's Consequences': The Effects of Cultural Values on Top Executive Commitment to the Status Quo," *Strategic Management Journal* (18:8), pp. 615-634.
- Geletkanycz, M. A., and Black, S. S. 2001. "Bound by the Past? Experience-Based effects on Commitment to the Strategic Status Quo," *Journal of Management* (27:1), pp. 3-21.
- Gemmo, V., Bissola, R., and Carignani, A. 2003. "Defining Prerequisites for Banking Web Site Design: The Wow! Approach," in *Proceedings of the 11th European Conference on Information Systems (ECIS)*, Naples, Italy, p. 12.
- Gerlach, J., Stock, R. M., and Buxmann, P. 2014. "Never Forget Where You're Coming from: The Role of Existing Products in Adoptions of Substituting Technologies," *Journal of Product Innovation Management* (31:S1), pp. 133-145.
- Gewald, H., and Dibbern, J. 2009. "Risks and Benefits of Business Process Outsourcing: A Study of Transaction Services in the German Banking Industry," *Information & Management* (46:4), pp. 249-257.



- Gigerenzer, G. 2004. "Dread Risk, September 11, and Fatal Traffic Accidents," *Psychological Science* (15:4), pp. 286-287.
- Goodhue, D. L., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management* (20:1), pp. 13-27.
- Gouscos, D., Kalikakis, M., and Georgiadis, P. 2003. "An Approach to Modeling Web Service QoS and Provision Price," in *Proceeding of the 4th International Conference on Web Information Systems Engineering Workshops*, Rome, Italy, pp. 121-130.
- Guardian 2015. "How Secure Is Your Smartphone?" <http://www.theguardian.com/media-network/2015/sep/29/how-secure-is-your-smartphone>. Accessed 19/04/2016.
- Guardian 2016. "Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History." <https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached>. Accessed 12/13/2017.
- Guardian 2017. "Uber Concealed Massive Hack that Exposed Data of 57m Users and Drivers." <https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack>. Accessed 12/13/2017.
- Haeussinger, F., and Kranz, J. 2013. "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior," in *Proceedings of the 34th International Conference on Information Systems (ICIS)*, Milan, Italy, p. 9.
- Haeussinger, F., and Kranz, J. 2017. "Antecedents of Employees' Information Security Awareness – Review, Synthesis, and Directions for Future Research," in *Proceedings of the 25th European Conference on Information Systems (ECIS)*, Guimarães, Portugal, p. 12.
- Hair, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2013. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Los Angeles, CA: Sage.
- Hair, J. F., Ringle, C., and Sarstedt, M. 2011. "PLS-SEM: Indeed a Silver Bullet," *Journal of Marketing Theory and Practice* (19:2), pp. 139-152.
- Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A. 2012. "An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research," *Journal of the Academy of Marketing Science* (40:3), pp. 414-433.

- Harris, C. R., Jenkins, M., and Glaser, D. 2006. "Gender Differences in Risk Assessment: Why Do Women Take Fewer Risks than Men?," *Judgment and Decision Making* (1:1), pp. 48-63.
- Herath, T., and Rao, H. R. 2009a. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.
- Herath, T., and Rao, H. R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.
- Hersch, J. 1996. "Decisions: Differences by Gender and Race," *Managerial and Decision Economics* (17:5), pp. 471-481.
- Hoffer, J. A., and Straub, D. W. 1994. "The 9 to 5 Underground: Are You Policing Computer Crimes?," in *Management of Information Systems*, P. Gray, W.R. King, E.R. Mclean and H. Watson (eds.). Fort Worth, TX: Harcourt Brace, pp. 388-401.
- Hoffman, L. W. 1972. "Early Childhood Experiences and Women's Achievement Motives," *Journal of Social Issues* (28:2), pp. 129-155.
- Homburg, C., Koschate, N., and Hoyer, W. D. 2005. "Do Satisfied Customers Really Pay More? A Study of the Relationship Between Customer Satisfaction and Willingness to Pay," *Journal of Marketing* (69:2), pp. 84-96.
- Hoorens, V. 1996. "Self-Favoring Biases for Positive and Negative Characteristics: Independent Phenomena?," *Journal of Social and Clinical Psychology* (15:1), pp. 53-67.
- Hsu, C. S., Chou, S.-W., and Min, H.-T. 2015. "Understanding Clients' Intentions to Explore Software-as-a-Service (SaaS) Features: A Social Capital Theory Perspective," in *Proceedings of the 19th Pacific Asia Conference on Information Systems (PACIS)*, Singapore, Singapore, p. 24.
- Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp. 615-660.

- Hu, Q., Hart, P., and Cooke, D. 2007. "The Role of External and Internal Influences on Information Systems Security – A Neo-Institutional Perspective," *The Journal of Strategic Information Systems* (16:2), pp. 153-172.
- Hulland, J. 1999. "Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies," *Strategic Management Journal* (20:2), pp. 195-204.
- IBM 2016. "10 Key Marketing Trends for 2017." <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN>. Accessed 11/01/2017.
- IDC 2014a. "Executive Summary: Data Growth, Business Opportunities, and the IT Imperatives." <https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>. Accessed 10/11/2017.
- IDC 2014b. "IDC 50th Anniversary – Transformation Everywhere." [https://www.idc.com/IDC\\_50anniversary/download/IDC50thAnniversary.pdf](https://www.idc.com/IDC_50anniversary/download/IDC50thAnniversary.pdf). Accessed 14/04/2017.
- IDC 2016. "Worldwide Public Cloud Services Spending Forecast to Double by 2019, According to IDC." <https://www.idc.com/getdoc.jsp?containerId=prUS40960516>. Accessed 11/11/2016.
- Isomäki, H., and Bilozarov, O. 2012. "Managers' Information Security Awareness in Russian ICT Small and Medium Sized Enterprises," in: *Proceedings of the 1st Information System Research Seminar in Scandinavia*. Sigtuna, Sweden: p. 35.
- Ittner, C. D., and Larcker, D. F. 1998. "Are Nonfinancial Measures Leading Indicators of Financial Performance? An Analysis of Customer Satisfaction," *Journal of Accounting Research* (36:Supplement), pp. 1-35.
- Johnson, J., Wilke, A., and Weber, E. U. 2004. "Beyond a Trait View of Risk Taking: A Domain-Specific Scale Measuring Risk Perceptions, Expected Benefits, and Perceived-Risk Attitudes in German-Speaking Populations," *Polish Psychological Bulletin* (35:3), pp. 153-172.
- Johnson, M. E., and Goetz, E. 2007. "Embedding Information Security into the Organization," *Security & Privacy, IEEE* (5:3), pp. 16-24.
- Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

- Kahneman, D., Knetsch, J. L., and Thaler, R. H. 1991. "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias," *The Journal of Economic Perspectives* (5:1), pp. 193-206.
- Kahneman, D., and Tversky, A. 1979. "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* (47:2), pp. 263-291.
- Kahneman, D., and Tversky, A. 1984. "Choices, Values, and Frames," *American Psychologist* (39:4), p. 341.
- Kajava, J., Anttila, J., Varonen, R., Savola, R., and Rönning, J. 2007. "Senior Executives Commitment to Information Security – From Motivation to Responsibility," in *Computational Intelligence and Security*. Springer, pp. 833-838.
- Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.
- Kano, N., Seraku, F., Takahashi, F., and Tsuji, S. 1984. "Attractive Quality and Must-be Quality," *The Journal of the Japanese Society for Quality Control* (14:2), pp. 39-48.
- Kaspersky 2014. "Android Mobile Security Threats." <https://usa.kaspersky.com/internet-security-center/threats/mobile#.Vwo7rXo6BU4>. Accessed 19/04/2016.
- Kim, H.-W., Chan, H. C., and Gupta, S. 2007. "Value-Based Adoption of Mobile Internet: An Empirical Investigation," *Decision Support Systems* (43:1), pp. 111-126.
- Kim, H.-W., and Kankanhalli, A. 2009. "Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective.," *MIS Quarterly* (33:3), pp. 567-582.
- Knapp, K. J., Marshall, T. E., Kelly Rainer, R., and Nelson Ford, F. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security* (14:1), pp. 24-36.
- Kotulic, A. G., and Clark, J. G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), pp. 597-607.
- Krasnova, H., Günther, O., Spiekermann, S., and Koroleva, K. 2009. "Privacy Concerns and Identity in Online Social Networks," *Identity in the Information Society* (2:1), pp. 39-63.

- Kritzinger, E., and Smith, E. 2008. "Information Security Management: An Information Security Retrieval and Awareness Model for Industry," *Computers & Security* (27:5), pp. 224-231.
- Kuan, K. K., and Chau, P. Y. 2001. "A Perception-based Model for EDI Adoption in Small Businesses Using a Technology–Organization–Environment Framework," *Information & Management* (38:8), pp. 507-521.
- Lacity, M. C., Khan, S. A., and Willcocks, L. P. 2009. "A Review of the IT Outsourcing Literature: Insights for Practice," *The Journal of Strategic Information Systems* (18:3), pp. 130-146.
- Landis, J. R., and Koch, G. G. 1977. "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33:1), pp. 159-174.
- Langer, E. J. 1975. "The Illusion of Control," *Journal of Personality and Social Psychology* (32:2), pp. 311-328.
- Lazarus, R. S., and Folkman, S. 1984. *Stress, Appraisal, and Coping*. New York: Springer Publishing Company.
- Lee, A. S. 1999. *Research MIS*. Oxford: Oxford University Press.
- Lee, D., Larose, R., and Rifon, N. 2008. "Keeping Our Network Safe: A Model of Online Protection Behaviour," *Behaviour & Information Technology* (27:5), pp. 445-454.
- Lee, M.-C. 2009. "Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefits," *Electronic Commerce Research and Applications* (8:3), pp. 130-141.
- Lee, S.-G., Chae, S. H., and Cho, K. M. 2013. "Drivers and Inhibitors of SaaS Adoption in Korea," *International Journal of Information Management* (33:3), pp. 429-440.
- Lee, Y., and Larsen, K. R. 2009. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2), pp. 177-187.
- Lengua, L. J., Sandler, I. N., West, S. G., Wolchik, S. A., and Curran, P. J. 1999. "Emotionality and Self-Regulation, Threat Appraisal, and Coping in Children of Divorce," *Development and Psychopathology* (11:01), pp. 15-37.
- Lenney, E. 1977. "Women's Self-Confidence in Achievement Settings," *Psychological Bulletin* (84:1), pp. 1-13.

- Levy, A. G., and Baron, J. 2005. "How Bad Is a 10% Chance of Losing a Toe? Judgments of Probabilistic Conditions by Doctors and Laypeople," *Memory & Cognition* (33:8), pp. 1399-1406.
- Levy, J. S. 1997. "Prospect Theory, Rational Choice, and International Relations," *International Studies Quarterly* (41:1), pp. 87-112.
- Li, N., and Kirkup, G. 2007. "Gender and Cultural Differences in Internet Use: A Study of China and the UK," *Computers & Education* (48:2), pp. 301-317.
- Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.
- Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.
- Liebermann, Y., and Stashevsky, S. 2002. "Perceived Risks as Barriers to Internet and E-commerce Usage," *Qualitative Market Research: An International Journal* (5:4), pp. 291-300.
- Lin, A., and Chen, N.-C. 2012. "Cloud Computing as an Innovation: Perception, Attitude, and Adoption," *International Journal of Information Management* (32:6), pp. 533-540.
- Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-sectional Research Designs," *Journal of Applied Psychology* (86:1), pp. 114-121.
- Loske, A., Widjaja, T., and Buxmann, P. 2013. "Cloud Computing Providers' Unrealistic Optimism regarding IT Security Risks: A Threat to Users?," in *Proceedings of the 34th International Conference on Information Systems (ICIS)*, Milan, Italy, p. 11.
- Luo, X., Li, H., Zhang, J., and Shim, J. P. 2010. "Examining Multi-Dimensional Trust and Multi-Faceted Risk in Initial Acceptance of Emerging Technologies: An Empirical Study of Mobile Banking Services," *Decision Support Systems* (49:2), pp. 222-234.
- Ma, Q., and Ratnasingam, P. 2008. "Factors Affecting the Objectives of Information Security Management," in *Proceedings of the 1st International Conference on Information Resources Management*, Ontario, Canada, p. 29.

- Matzler, K., Bailom, F., Hinterhuber, H. H., Renzl, B., and Pichler, J. 2004a. "The Asymmetric Relationship Between Attribute-level Performance and Overall Customer Satisfaction: A Reconsideration of the Importance–Performance Analysis," *Industrial Marketing Management* (33:4), pp. 271-277.
- Matzler, K., Fuchs, M., and Schubert, A. 2004b. "Employee Satisfaction: Does Kano's Model Apply?," *Total Quality Management and Business Excellence* (15:9-10), pp. 1179-1198.
- Matzler, K., and Hinterhuber, H. H. 1998. "How to Make Product Development Projects More Successful by Integrating Kano's Model of Customer Satisfaction into Quality Function Deployment," *Technovation* (18:1), pp. 25-38.
- Mayer, J. H. 2012. "Using The Kano Model To Identify Attractive User-Interface Software Components," in *Proceedings of the 33rd International Conference on Information Systems (ICIS)*, Orlando, USA, p. 2.
- McKenna, F. P. 1993. "It Won't Happen to Me: Unrealistic Optimism or Illusion of Control?," *British Journal of Psychology* (84:1), pp. 39-50.
- McLellan, C. 2016. "SaaS in 2016: The Key Trends." <http://www.zdnet.com/article/saas-in-2016-the-key-trends/>. Accessed 04/14/2017.
- Mette, P., Moser, F., and Fridgen, G. 2013. "A Quantitative Model for Using Open Innovation in Mobile Service Development," in: *Wirtschaftsinformatik Proceedings*. p. 5.
- Miles, M. B., and Huberman, A. M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. London, United Kingdom: SAGE Publications.
- Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology* (7:2), pp. 163-184.
- Mingers, J. 2001. "Combining IS Research Methods: Towards a Pluralist Methodology," *Information Systems Research* (12:3), pp. 240-259.
- Minton, H. L., and Schneider, F. W. 1985. *Differential Psychology*. Prospect Heights: Waveland Press.
- Mittal, V., Anderson, E. W., Sayrak, A., and Tadikamalla, P. 2005. "Dual Emphasis and the Long-Term Financial Impact of Customer Satisfaction," *Marketing Science* (24:4), pp. 544-555.

- Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192-222.
- Moqbel, M. A., and Bartelt, V. L. 2015. "Consumer Acceptance of Personal Cloud: Integrating Trust and Risk with the Technology Acceptance Model," *AIS Transactions on Replication Research* (1:1), pp. 1-11.
- Mouratidis, H., Jahankhani, H., and Nkhoma, M. Z. 2008. "Management Versus Security Specialists: An Empirical Study on Security Related Perceptions," *Information Management & Computer Security* (16:2), pp. 187-205.
- Myers, M. D. 1997. "Qualitative Research in Information Systems," *MIS Quarterly* (21:2), pp. 241-242.
- Narain Singh, A., Gupta, M. P., and Ojha, A. 2014. "Identifying Factors of "Organizational Information Security Management," *Journal of Enterprise Information Management* (27:5), pp. 644-667.
- Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.
- Ng, B. Y., and Feng, A. E. 2006. "An Exploratory Study on Managerial Security Concerns in Technology Start-ups," in *Proceedings of the 10th Pacific Asia Conference on Information Systems (PACIS)*, Kuala Lumpur, Malaysia, p. 29.
- Nilsson-Witell, L., and Fundin, A. 2005. "Dynamics of Service Attributes: A Test of Kano's Theory of Attractive Quality," *International Journal of Service Industry Management* (16:2), pp. 152-168.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126.
- NowSecure 2016. "Mobile Security Report." <https://info.nowsecure.com/rs/201-XEW-873/images/2016-NowSecure-mobile-security-report.pdf>. Accessed 08/21/2016.
- Nunnally, J. C. 1978. *Psychometric Theory*. New York: McGraw-Hill.
- Nunnally, J. C., Bernstein, I. H., and Berge, J. M. t. 1967. *Psychometric Theory*. New York, USA: McGraw-Hill.



- Oliver, R. L. 1980. "A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions," *Journal of Marketing Research* (17:4), pp. 460-469.
- OTA 2016. "2016 Data Protection & Breach Readiness Guide." [https://otalliance.org/system/files/files/resource/documents/2016breachguide\\_0.pdf](https://otalliance.org/system/files/files/resource/documents/2016breachguide_0.pdf). Accessed 05/03/2017.
- Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Science (HICSS)*, Waikoloa, HI, USA, p. 156b.
- Pajares, F. 2002. "Gender and Perceived Self-Efficacy in Self-Regulated Learning," *Theory Into Practice* (41:2), pp. 116-125.
- Patrick, B. C., Skinner, E. A., and Connell, J. P. 1993. "What Motivates Children's Behavior and Emotion? Joint Effects of Perceived Control and Autonomy in the Academic Domain," *Journal of Personality and Social Psychology* (65:4), pp. 781-791.
- Pearlin, L. I., and Schooler, C. 1978. "The Structure of Coping," *Journal of Health and Social Behavior* (19:1), pp. 2-21.
- Peltier, T. R. 2005. "Implementing an Information Security Awareness Program," *Information Systems Security* (14:2), pp. 37-49.
- Perloff, L. S., and Fetzer, B. K. 1986. "Self-Other Judgments and Perceived Vulnerability to Victimization," *Journal of Personality and Social Psychology* (50:3), p. 502.
- Perrin, C. 2008. "The CIA Triad." Retrieved from <http://www.techrepublic.com/blog/security/the-ciatriad/488>. Accessed 10/19/2017.
- Plott, C. R., and Zeiler, K. 2005. "The Willingness to Pay-Willingness to Accept Gap, the Endowment Effect, Subject Misconceptions, and Experimental Procedures for Eliciting Valuations," *American Economic Review* (95:3), pp. 530-545.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.
- Polites, G. L., and Karahanna, E. 2012. "Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance," *MIS Quarterly* (36:1), pp. 21-42.

- Posthumus, S., and Von Solms, R. 2004. "A Framework for the Governance of Information Security," *Computers & Security* (23:8), pp. 638-646.
- Preacher, K. J., and Hayes, A. F. 2008. "Asymptotic and Resampling Strategies For Assessing and Comparing Indirect Effects in Multiple Mediator Models," *Behavior Research Methods* (40:3), pp. 879-891.
- Prentice-Dunn, S., and Rogers, R. W. 1986. "Protection Motivation Theory and Preventive Health: Beyond the Health Belief Model," *Health Education Research* (1:3), pp. 153-161.
- Prentice, D. A., and Carranza, E. 2002. "What Women and Men Should Be, Shouldn't Be, Are Allowed to Be, and Don't Have to Be: The Contents of Prescriptive Gender Stereotypes," *Psychology of Women Quarterly* (26:4), pp. 269-281.
- Ptacek, J. T., Smith, R. E., and Zanas, J. 1992. "Gender, Appraisal, and Coping: A Longitudinal Analysis," *Journal of Personality* (60:4), pp. 747-770.
- Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757-778.
- pwc 2015. "The Global State of Information Security Survey." <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>. Accessed 06/08/2015.
- Quan-Haase, A., and Young, A. L. 2010. "Uses and Gratifications of Social Media: A Comparison of Facebook and Instant Messaging," *Bulletin of Science, Technology & Society* (30:5), pp. 350-361.
- Rhee, H.-S., Ryu, Y., and Kim, C.-T. 2005. "I Am Fine But You Are Not: Optimistic Bias and Illusion of Control on Information Security," in *Proceedings of the 26th International Conference on Information Systems (ICIS)*, Las Vegas, USA, p. 32.
- Rhee, H.-S., Ryu, Y. U., and Kim, C.-T. 2012. "Unrealistic Optimism on Information Security Management," *Computers & Security* (31:2), pp. 221-232.
- Rivera, J., and van der Meulen, R. 2014. "Gartner Survey Reveals That SaaS Deployments Are Now Mission Critical," in: *Survey Reveals Enterprise Cloud Adoption Plans Through 2017*. Stamford: Gartner.
- Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), pp. 93-114.

- Roodhooft, F., and Warlop, L. 1999. "On the Role of Sunk Costs and Asset Specificity in Outsourcing Decisions: A Research Note," *Accounting, Organizations and Society* (24:4), pp. 363-369.
- Roster, C. A., and Richins, M. L. 2009. "Ambivalence and Attitudes in Consumer Replacement Decisions," *Journal of Consumer Psychology* (19:1), pp. 48-61.
- Ruighaver, A. B., Maynard, S. B., and Chang, S. 2007. "Organisational Security Culture: Extending the End-User Perspective," *Computers & Security* (26:1), pp. 56-62.
- Rustagi, S., King, W. R., and Kirsch, L. J. 2008. "Predictors of Formal Control Usage in IT Outsourcing Partnerships," *Information Systems Research* (19:2), pp. 126-143.
- Sakao, T. 2009. "Quality Engineering for Early Stage of Environmentally Conscious Design," *The Total Quality Management Journal* (21:2), pp. 182-193.
- Saldaña, J. 2015. *The Coding Manual for Qualitative Researchers*. London, United Kingdom: Sage.
- Samuelson, W., and Zeckhauser, R. 1988. "Status Quo Bias in Decision Making," *Journal of Risk and Uncertainty* (1:1), pp. 7-59.
- Sarstedt, M., Henseler, J., and Ringle, C. M. 2011. "Multigroup Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results," in *Measurement and Research Methods in International Marketing (Advances in International Marketing)* M. Sarstedt, M. Schwaiger and C.R. Taylor (eds.). Bingley, United Kingdom: Emerald Group Publishing Limited, pp. 195-218.
- Sauerwein, E., Bailom, F., Matzler, K., and Hinterhuber, H. H. 1996. "The Kano Model: How to delight your Customers," in: *IX. International Working Seminar on Production Economics*. Innsbruck: pp. 313-327.
- Saunders, C. S., and Clark, S. 1992. "EDI Adoption and Implementation: A Focus on Interorganizational Linkages," *Information Resources Management Journal* (5:1), pp. 9-20.
- Schwarz, N. 1999. "Self-Reports: How the Questions Shape the Answers," *American Psychologist* (54:2), pp. 93-105.
- Schweitzer, M. 1995. "Multiple Reference Points, Framing, and the Status Quo Bias in Health Care Financing Decisions," *Organizational Behavior and Human Decision Processes* (63:1), pp. 69-72.

- Schwenk, C. 1984. "Cognitive Simplification Processes in Strategic Decision-Making: Insights from Behavioral Decision Theory and Cognitive Psychology," *Strategic Management Journal* (5:2), pp. 111-128.
- Seder, A. M., and Alhazza, M. H. F. 2014. "Review on the Theory Of Attractive Quality Kano Model," *Journal of Advanced Science and Engineering Research Vol* (4:2), pp. 88-102.
- Shameli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M. 2016. "Taxonomy of Information Security Risk Assessment (ISRA)," *Computers & Security* (57:March), pp. 14-30.
- Sharma, R., and Yetton, P. 2007. "The Contingent Effects of Training, Technical Complexity, and Task Interdependence on Successful Information Systems Implementation," *MIS Quarterly* (31:2), pp. 219-238.
- Sheeran, P. 2002. "Intention-Behavior Relations: A Conceptual and Empirical Review," *European Review of Social Psychology* (12:1), pp. 1-36.
- Shepperd, J. A., Carroll, P., Grace, J., and Terry, M. 2002. "Exploring the Causes of Comparative Optimism," *Psychologica Belgica* (42:1/2), pp. 65-98.
- Shin, D.-H. 2010. "The Effects of Trust, Security and Privacy in Social Networking: A Security-Based Approach to Understand the Pattern of Adoption," *Interacting with computers* (22:5), pp. 428-438.
- Shoham, A., and Fiegenbaum, A. 2002. "Competitive Determinants of Organizational Risk-Taking Attitude: The Role of Strategic Reference Points," *Management Decision* (40:2), pp. 127-141.
- Sinha, T. 1994. "Prospect Theory and the Risk Return Association: Another Look," *Journal of Economic Behavior & Organization* (24:2), pp. 225-231.
- Siponen, M. 2001. "Five Dimensions of Information Security Awareness," *Computers and Society* (31:2), pp. 24-29.
- Siponen, M. 2006. "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems* (7:1), p. 19.
- Siponen, M., Pahlila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64-71.

- Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.
- Siponen, M. T. 2000a. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), pp. 31-41.
- Siponen, M. T. 2000b. "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice," *Information Management & Computer Security* (8:5), pp. 197-209.
- Skycure 2015. "Skycure Study: 2015 Best & Worst Tourist Attractions for Mobile Security." <https://www.skycure.com/blog/skycure-study-2015-best-worst-tourist-attractions-for-mobile-security/>. Accessed 08/21/2016.
- Slovic, P. 1975. "Choice Between Equally-Valued Alternatives," *Journal of Experimental Psychology* (1:3), pp. 280-287.
- Slovic, P. 1987. "Perception of Risk," *Science, New Series* (236:4799), pp. 280-285.
- SmartPLS 2016. "SmartPLS 3.2.4." <https://www.smartpls.com/>. Accessed 08/25/2016.
- Smetters, D. K., and Grinter, R. E. 2002. "Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications," in: *Proceedings of the Workshop on New Security Paradigms*. Virginia Beach, USA: pp. 82-89.
- Smith, G. F. 1992. "Towards a Theory of Managerial Problem Solving," *Decision Support Systems* (8:1), pp. 29-40.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.
- Socialnomics 2016. "6 Cyber Security Statistics You Should Know for 2016." <http://socialnomics.net/2016/08/17/6-cyber-security-statistics-you-should-know-for-2016/>. Accessed 05/03/2017.
- Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 42-75.
- Sonnenreich, W., Albanese, J., and Stout, B. 2006. "Return on Security Investment (ROSI) - A Practical Quantitative Model," *Journal of Research and Practice in Information Technology* (38:1), pp. 45-56.

- Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.
- Statista 2017a. "Size of the Cyber Security Market Worldwide, from 2016 to 2021." <https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/>. Accessed 11/23/2017.
- Statista 2017b. "Welche Treiber führen Ihrer Meinung nach zur Veränderungen in der IT-Sicherheit?" <https://de.statista.com/statistik/daten/studie/384321/umfrage/umfrage-zu-treibern-der-veraenderung-in-der-it-sicherheit/>. Accessed 11/23/2017.
- Stone, A. A., and Neale, J. M. 1984. "New Measure of Daily Coping: Development and Preliminary Results," *Journal of Personality and Social Psychology* (46:4), pp. 892-906.
- Stoneburner, G., Goguen, A. Y., and Feringa, A. 2002. "Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology," <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
- Straub, D. W., and Welke, R. J. 1998. "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.
- Synergy 2016. "2015 Review Shows \$110 Billion Cloud Market Growing at 28% Annually." <https://www.srgresearch.com/articles/2015-review-shows-110-billion-cloud-market-growing-28-annually>. Accessed 11/11/2016.
- Szmigin, I., and Reppel, A. E. 2004. "Internet Community Bonding: The Case of Macnews.de," *European Journal of Marketing* (38:5/6), pp. 626-640.
- Tamres, L. K., Janicki, D., and Helgeson, V. S. 2002. "Sex Differences in Coping Behavior: A Meta-Analytic Review and an Examination of Relative Coping," *Personality and Social Psychology Review* (6:1), pp. 2-30.
- Tan, K. C., and Shen, X.-X. 2000. "Integrating Kano's Model in the Planning Matrix of Quality Function Deployment," *Total Quality Management* (11:8), pp. 1141-1151.
- The Wall Street Journal 2016. "IRS Says Cyberattacks on Taxpayer Accounts More Extensive Than Previously Reported." <https://www.wsj.com/articles/irs-says-cyberattacks-on-taxpayer-accounts-more-extensive-than-previously-reported-1456514909>. Accessed 05/03/2017.

- Thomas, D. M., and Watson, R. T. 2002. "Q-Sorting and MIS Research: A Primer," *Communications of the Association for Information Systems* (8:1), p. 9.
- Thomson, M. E., and von Solms, R. 1998. "Information Security Awareness: Educating Your Users Effectively," *Information Management & Computer Security* (6:4), pp. 167-173.
- Trauth, E. M. 2013. "The Role of Theory in Gender and Information Systems Research," *Information and Organization* (23:4), pp. 277-293.
- Trauth, E. M., Joshi, K. D., Kvasny, L., Chong, J., Kulturel-Konak, S., and Mahar, J. 2010. "Millennials and Masculinity: A Shifting Tide of Gender Typing of ICT?," in *Proceedings of the 16th Americas Conference on Information Systems (AMCIS)*, Lima, Peru, p. 73.
- Tversky, A., and Kahneman, D. 1975. "Judgment Under Uncertainty: Heuristics and Biases," in *Utility, Probability, and Human Decision Making*, D. Wendt and C. Vlek (eds.). Dordrecht, Holland: Springer Netherlands, pp. 141-162.
- Tversky, A., and Kahneman, D. 1985. "The Framing of Decisions and the Psychology of Choice," in *Environmental Impact Assessment, Technology Assessment, and Risk Analysis*, V.T. Covello, J.L. Mumpower, P.J.M. Stallen and V.R.R. Uppuluri (eds.). Springer-Verlag Berlin Heidelberg, pp. 107-129.
- Uffen, J., Guhr, N., and Breitner, M. H. 2012. "Personality Traits and Information Security Management: An Empirical Study of Information Security Executives," in *Proceedings of the 33rd International Conference on Information Systems (ICIS)*, Orlando, USA, p.5.
- van der Meulen, R., and Rivera, J. 2015. "Gartner Says Cloud Is a Viable Option, But Not a Top Consideration for Many CIOs," in: *I&O Leaders Should Institute a "Cloud-First" Consideration for Every Project on an Application-by-Application Basis*, Gartner (ed.). Stamford.
- Van Niekerk, J., and Von Solms, R. 2010. "Information Security Culture: A Management Perspective," *Computers & Security* (29:4), pp. 476-486.
- Vance, A., Anderson, B. B., Kirwan, C. B., and Eargle, D. 2014. "Using Measures of Risk Perception to Predict Information Security Behavior: Insights From Electroencephalography (EEG)," *Journal of the Association for Information Systems* (15:10), pp. 679-722.

- Vance, A., Siponen, M., and Pahnla, S. 2012. "Motivating IS Security Compliance: Insights From Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190-198.
- Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21-54.
- Venkatesh, V., and Morris, M. G. 2000. "Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and their Role in Technology Acceptance and Usage Behavior," *MIS Quarterly* (24:1), pp. 115-139.
- Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.
- Vetter, J., Benlian, A., and Hess, T. 2011. "Setting Targets Right! How Non-Rational Biases Affect the Risk Preference of IT-Outsourcing Decision Makers - An Empirical Investigation," in *Proceedings of 19th the European Conference of Information Systems (ECIS)*, Helsinki, Finland, p. 173.
- Virtru 2015. "4 Data Breaches That Would've Been Prevented by Encrypted Email." <https://www.virtu.com/blog/data-breaches/>. Accessed 05/03/2017.
- Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. 2009. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," in *Proceedings of the 17th European Conference on Information Systems (ECIS)*, Verona, Italy, pp. 2206-2217.
- Wang, T., and Hsu, C. 2010. "The Impact of Board Structure on Information Security Breaches," in *Proceedings of the 14th Pacific Asia Conference on Information Systems (PACIS)*, Taipei, Taiwan, p. 165.
- Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. Xiii-Xxiii.
- Weinstein, N. D. 1980. "Unrealistic Optimism about Future Life Events," *Journal of Personality and Social Psychology* (39:5), pp. 806-820.
- Weinstein, N. D. 1982. "Unrealistic Optimism About Susceptibility to Health Problems," *Journal of Behavioral Medicine* (5:4), pp. 441-460.



- Weinstein, N. D. 1993. "Testing Four Competing Theories of Health-Protective Behavior," *Health Psychology* (12:4), pp. 324-333.
- Weinstein, N. D., and Klein, W. M. 1996. "Unrealistic Optimism: Present and Future," *Journal of Social and Clinical Psychology* (15:1), pp. 1-8.
- Whitman, M. E. 2004. "In Defense of the Realm: Understanding the Threats to Information Security," *International Journal of Information Management* (24:1), pp. 43-57.
- Willcocks, L., Fitzgerald, G., and Lacity, M. 1996. "To Outsource IT or Not?: Recent Research on Economics and Evaluation Practice," *European Journal of Information Systems* (5:3), pp. 143-160.
- Wills, T. A. 1981. "Downward Comparison Principles in Social Psychology," *Psychological Bulletin* (90:2), pp. 245-271.
- Wilson, M., and Daly, M. 1985. "Competitiveness, Risk Taking, and Violence: The Young Male Syndrome," *Ethology and Sociobiology* (6:1), pp. 59-73.
- Witte, K. 1992. "Putting the Fear Back Into Fear Appeals: The Extended Parallel Process Model," *Communications Monographs* (59:4), pp. 329-349.
- Witte, K. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communication* (1:4), pp. 317-342.
- Wood, J. V. 1989. "Theory and Research Concerning Social Comparisons of Personal Attributes," *Psychological Bulletin* (106:2), pp. 231-248.
- Woon, I., Tan, G.-W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the International Conference on Information Systems (ICIS)*, Las Vegas, USA, p. 31.
- Workman, M., Bommer, W. H., and Straub, D. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp. 2799-2816.
- World Economic Forum 2010. "Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-driven Transformation." <https://www.weforum.org/reports/exploring-future-cloud-computing-riding-next-wave-technology-driven-transformation>. Accessed 14/04/2017.

- Wu, J.-H., and Wang, S.-C. 2005. "What Drives Mobile Commerce? An Empirical Evaluation of the Revised Technology Acceptance Model," *Information & Management* (42:5), pp. 719-729.
- Wu, W.-W., Lan, L. W., and Lee, Y.-T. 2011. "Exploring Decisive Factors Affecting an Organization's SaaS Adoption: A Case Study," *International Journal of Information Management* (31:6), pp. 556-563.
- Wu, Y. A., and Saunders, C. S. 2005. "Decision Making, IT Governance, and Information Systems Security," in *Proceedings of the 11th Americas Conference on Information Systems (AMCIS)*, Omaha, USA, p. 459.
- Zajonc, R. B. 1968. "Attitudinal Effects of Mere Exposure," *Journal of Personality and Social Psychology* (9:2), pp. 1-27.
- Zhao, M., and Roy Dholakia, R. 2009. "A Multi-Attribute Model of Web Site Interactivity and Customer Satisfaction: An Application of the Kano Model," *Managing Service Quality: An International Journal* (19:3), pp. 286-307.
- Zhou, T. 2011. "The Impact of Privacy Concern on User Adoption of Location-based Services," *Industrial Management & Data Systems* (111:2), pp. 212-226.